

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 1)

(11) 特許番号

特許第3445986号
(P3445986)

(45) 発行日 平成15年 9 月16日 (2003. 9. 16)

(24) 登録日 平成15年 6 月27日 (2003. 6. 27)

(51) Int. Cl. ⁷	識別記号	F I
H 0 4 L 12/56		H 0 4 L 12/56 A
// G 0 6 F 13/00	3 5 1	G 0 6 F 13/00 3 5 1 Z
H 0 4 L 12/66		H 0 4 L 12/66 B

請求項の数26(全 19 頁)

(21) 出願番号 特願2002-283287(P2002-283287)

(22) 出願日 平成14年 9 月27日 (2002. 9. 27)

審査請求日 平成15年 3 月25日 (2003. 3. 25)

早期審査対象出願

(73) 特許権者 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 武知 秀明

大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(72) 発明者 加藤 尚徳

大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(72) 発明者 武田 英俊

大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(74) 代理人 100062144

弁理士 青山 葆 (外 1 名)

審査官 中木 努

最終頁に続く

(54) 【発明の名称】 インターネットに接続するサーバ、機器および通信システム

1

(57) 【特許請求の範囲】

【請求項 1】 インターネットに接続された少なくとも
1つの機器と、インターネットに接続可能な少なくとも
1つの端末との間の通信を転送する、インターネットに
接続されたサーバであって、

前記機器からの定期的な通知パケットを受信し、

前記端末からの前記機器に対する転送要求があった場

合、前記通知パケットの応答として接続要求パケットを
前記機器に送信し、

該接続要求パケットに応答して前記機器から前記サーバ 10
へ送信されたTCP接続要求を受諾し、

TCP接続確立後、そのTCP接続上で前記端末と前記
機器間の通信を転送することを特徴とするサーバ。

【請求項 2】 前記サーバは、前記端末から機器IDを
含んだHTTPリクエストにより前記機器に対する転送

2

要求を受信し、

前記端末と前記機器の間の通信の転送を、前記端末から
のHTTPリクエストを前記機器から張られたTCP接
続上に転送し、前記機器から前記TCP接続を通じて受
信したHTTPレスポンスを端末へ転送することにより
行なうことを特徴とする請求項 1 記載のサーバ。

【請求項 3】 前記サーバは、少なくとも 1つの端末か
ら複数の転送要求を受信することができ、前記端末から
前記機器に対する複数の転送要求があった場合に、各々
に一意なセッション識別子を生成して前記接続要求パケ
ットにより機器に通知し、

前記接続要求パケットに応答して前記機器から前記サー
バへ送信されたTCP接続要求を受諾してTCP接続を
確立し、該確立したTCP接続上で前記機器から送信さ
れるセッション識別子を受信し、そのTCP接続に前記

BEST AVAILABLE COPY

受信したセッション識別子を対応付けることで、前記端末からの複数の接続要求に対して複数のTCP接続を各々対応付け、

前記端末がセッション識別子を指定して接続を要求し、且つ、該指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合に、前記端末からの通信をその確立済みのTCP接続上で転送することにより、セッション識別子毎に並列して通信内容の転送を行うことを特徴とする請求項1記載のサーバ。

【請求項4】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時刻を記録する記憶手段を備え、前記機器からの定期的な通知パケットを受信したときに、前記最終アクセス時刻を該受信時刻で更新し、前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が所定期間を超えている場合は該接続要求を拒否し、その差が所定期間以下の場合は前記通知パケットの応答として接続要求パケットを前記機器に送ることを特徴とする請求項1記載のサーバ。

【請求項5】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、前記機器に予め最大アクセス確認周期情報を送信し、前記機器からの定期的な通知パケットを受信したときに、最終アクセス時刻を該通知パケットの受信時刻で更新し、前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が最大アクセス確認周期情報が示す値を超えた場合は、前記接続要求を拒否し、その差が最大アクセス確認周期情報が示す値以下の場合は、前記通知パケットの応答として接続要求パケットを前記機器に送ることを特徴とする請求項1記載のサーバ。

【請求項6】 前記サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備え、前記端末と前記機器の間で秘密情報を転送する際、予め前記端末にサーバ証明書を送信し、前記機器により確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記機器に送信し、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記端末に送信することを特徴とする請求項1記載のサーバ。

【請求項7】 前記サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備え、前記端末と前記機器の間で秘密情報を転送する際、予め前記端末と前記機器に各々サーバ証明書を送信し、

前記確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記機器に送信し、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記端末に送信することを特徴とする請求項1記載のサーバ。

【請求項8】 インターネットに接続されたサーバと通信する、インターネットに接続された機器であって、前記サーバに定期的に通知パケットを送信し、前記サーバから接続要求パケットを受信した場合、前記サーバに対してTCP接続要求を送信し、TCP接続後、そのTCP接続上で前記サーバと通信することを特徴とする機器。

【請求項9】 前記機器は、前記TCP接続上での前記サーバとの通信を、前記サーバからHTTPリクエストを受信し、前記サーバへHTTPレスポンスを送信することにより行なうことを特徴とする請求項8記載の機器。

【請求項10】 前記機器は、Webサーバモジュールと転送モジュールを備え、前記Webサーバモジュールは、前記転送モジュールからHTTPリクエストを受信してHTTPレスポンスを返信し、前記転送モジュールは、前記サーバから前記接続要求パケットを受信した際は前記サーバに対してTCP接続要求を送信してTCP接続を確立し、そのTCP接続上で前記サーバからHTTPリクエストを受信して前記Webサーバに転送し、前記WebサーバからHTTPレスポンスを受信して前記サーバに前記TCP接続上で転送することを特徴とする請求項9記載の機器。

【請求項11】 前記機器は、前記サーバからセッション識別子を伴った接続要求パケットを受信した場合、前記サーバに対してTCP接続を確立し、その確立したTCP接続上で前記セッション識別子をサーバに送信し、前記TCP接続確立後は、前記TCP接続上で前記サーバと通信することを特徴とする請求項8記載の機器。

【請求項12】 前記機器は、前記サーバから最大アクセス確認周期情報を予め受信して前記機器内に保存しておき、前記最大アクセス確認周期情報が示す周期より短い周期で定期的に通知パケットを送信することを特徴とする請求項8記載の機器。

【請求項13】 前記機器は、通信を暗号化および復号化する暗号通信手段を備え、前記サーバと秘密情報の送受信を確立したTCP接続上で暗号通信手段により暗号化して行うことを特徴とする請求項8記載の機器。

【請求項14】 前記機器は、サーバ証明書を検証する

手段と通信を暗号化および復号化する暗号通信手段を備え、

前記サーバからサーバ証明書を受信し、

前記サーバと秘密情報の送受信を、前記サーバ証明書を認証して正規であることを確認した後に前記確立したTCP接続上で暗号通信手段により暗号化して行うことを特徴とする請求項8記載の機器。

【請求項15】 インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を、インターネットに接続されたサーバを介して転送する通信システムであって、前記機器は前記サーバに定期的に通知バケットを送り、前記サーバは前記端末から前記機器に対する転送要求があった場合、前記通知バケットの応答として接続要求バケットを前記機器に送り、前記機器は、前記サーバから接続要求バケットを受信した場合、前記サーバに対してTCP接続要求を送信し、前記サーバは、前記接続要求バケットに応答して前記機器から前記サーバへ送信されたTCP接続要求を受諾し、これによりTCP接続を確立し、前記サーバは、前記TCP接続確立後、そのTCP接続上で前記端末と前記機器の間の通信を転送することを特徴とする通信システム。

【請求項16】 前記端末は前記サーバに対し機器IDを含んだHTTPリクエストを送信することにより前記機器に対する転送要求を行い、前記サーバは前記端末と前記機器の間の通信を転送する際に、前記端末からのHTTPリクエストを前記機器から張られたTCP接続上に転送し、前記機器は転送された前記HTTPリクエストを処理して、それに対するHTTPレスポンスを前記TCP接続上で前記サーバへ応答し、前記サーバは該HTTPレスポンスを端末へ転送することを特徴とする請求項15記載の通信システム。

【請求項17】 前記サーバは、少なくとも1つの端末から複数の転送要求を受信することができ、前記端末から前記機器に対する複数の転送要求があった場合に、各々に一意なセッション識別子を生成し、前記接続要求バケットにより前記機器に通知し、前記機器は、前記サーバからセッション識別子を伴った接続要求バケットを受信した場合、前記サーバに対してTCP接続を確立し、その確立したTCP接続上で前記セッション識別子をサーバに送信し、前記TCP接続確立後は、前記TCP接続上で前記サーバと通信し、前記サーバは、前記接続要求バケットに応答して前記機器から前記サーバへ送信されたTCP接続要求を受諾してTCP接続を確立し、前記TCP接続上で前記機器から送信されるセッション識別子を受信し、前記TCP接続に前記受信されたセッション識別子に対応付けることで、前記端末からの複数の接続要求に対して複数のTCP

P接続を各々対応付け、

前記サーバは、前記端末がセッション識別子を指定して接続を要求し、且つ、該指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合、前記確立済みのTCP接続上で前記端末からの通信を転送することにより、セッション識別子毎に並列して通信内容の転送を行うことを特徴とする請求項15記載の通信システム。

【請求項18】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、前記サーバは、前記機器に予め最大アクセス確認周期情報を送信し、前記機器は、その最大アクセス確認周期情報を受信して内部に保存しておき、前記最大アクセス確認周期情報が示す周期よりも短い周期で定期的に通知バケットを送信し、前記サーバは、前記機器から通知バケットを受信した際に最終アクセス時刻を通知バケットの受信時刻で更新し、

前記サーバは、前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が最大アクセス確認周期情報が示す周期を超えている場合は前記接続要求を拒否し、その差が最大アクセス確認周期情報が示す周期以下の場合は、前記通知バケットの応答として接続要求バケットを前記機器に送信することを特徴とする請求項15記載の通信システム。

【請求項19】 前記サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備え、

前記端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段とを備え、前記機器は、通信を暗号化および復号化する暗号通信手段を備え、前記サーバは、前記端末と前記機器の間で秘密情報を転送する際、予め前記端末にサーバ証明書を送信し、前記端末は、前記サーバと秘密情報の送受信を、前記サーバ証明書を認証して正規であることを確認した後に暗号通信手段により暗号化して行い、前記機器は、前記サーバと秘密情報の送受信を、前記確立されたTCP接続で暗号通信手段により暗号化して行い、前記サーバは、前記確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記機器に送信し、前記サーバは、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号

化して前記端末に送信することを特徴とする請求項15記載の通信システム。

【請求項20】 前記サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備え、

前記端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備え、

前記機器は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備え、

前記サーバは、前記端末と前記機器の間に秘密情報を転送する際、予め前記端末と前記機器に各々サーバ証明書を送信し、

前記端末は、前記サーバと秘密情報の送受信を、前記サーバ証明書を認証して正規であることを確認した後に暗号通信手段により暗号化して行い、

前記機器は、前記サーバと秘密情報の送受信を、前記サーバ証明書を認証して正規であることを確認した後に前記機器が確立したTCP接続上で暗号通信手段により暗号化して行い、

前記サーバは、前記機器により確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記機器に送信し、

前記サーバは、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記端末に送信することを特徴とする請求項15記載の通信システム。

【請求項21】 インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を転送する、インターネットに接続されたサーバであって、

複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、

前記機器から第1及び第2の通知バケットを定期的を受信し、

前記機器から第1の通知バケットを受信したときは、最終アクセス時刻を受信時刻で更新し、前記機器から第2の通知バケットを受信したときは、最終アクセス時刻を更新せず、

前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が所定期間を超えている場合は前記接続要求を拒否し、その差が所定期間以下の場合は前記第1及び第2の通知バケットの応答として接続要求バケットを前記機器に送り、前記接続要求バケットに応答して前記機器から前記サーバへ送信されるTCP接続要求を受諾し、

TCP接続確立後は、前記TCP接続上で前記端末と前

記機器の間の通信を転送することを特徴とするサーバ。

【請求項22】 インターネットに接続されたサーバと通信する、インターネットに接続された機器であって、前記サーバに第1及び第2の通知バケットを定期的を送信し、前記第1の通知バケットの送信周期は前記第2の通知バケットの送信周期より長く、

前記機器は、前記サーバから接続要求バケットを受信した場合、前記サーバに対してTCP接続要求を送信し、前記機器はTCP接続が確立後、前記TCP接続上で前記サーバと通信することを特徴とする機器。

【請求項23】 インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を、インターネットに接続されたサーバが転送する通信システムであって、

前記サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、

前記機器は、前記サーバに第1及び第2の通知バケットを定期的を送り、前記第1の通知バケットの送信周期は前記第2の通知バケットの送信周期よりも長く、

前記サーバは、機器から第1及び第2の通知バケットを受信し、前記機器から第1の通知バケットを受信したときに最終アクセス時刻を受信時刻で更新し、第2の通知バケットを受信したときには最終アクセス時刻を更新せず、

前記サーバは、前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が所定期間を超えている場合は前記接続要求を拒否し、その差が所定期間以下の場合は、前記第1及び第2の通知バケットの応答として接続要求バケットを前記機器に送り、

前記機器は、前記サーバから接続要求バケットを受信した場合、前記サーバに対してTCP接続要求を送信し、前記サーバは、前記接続要求バケットに応答して前記機器から前記サーバへ送信されたTCP接続要求を受諾し、これによりTCP接続を確立し、

前記サーバは、前記TCP接続が確立後、そのTCP接続上で前記端末と前記機器の間の通信を転送することを特徴とする通信システム。

【請求項24】 プログラム可能な装置を、請求項1ないし7のいずれか一つ又は21に記載のサーバとして動作させるためのプログラム。

【請求項25】 プログラム可能な装置を、請求項8ないし14のいずれか一つ又は22に記載の機器として動作させるためのプログラム。

【請求項26】 請求項24又は25に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、IPプロトコルを採用する通信システムであって、特に、インターネット

上の機器から所望のタイミングでルータを介してローカルエリアネットワーク内の機器に対する通信を開始できる通信システムに関する。

【0002】

【従来の技術】近年、企業、家庭を問わず、Network Address Translation機能（以下「NAT」と称す。）またはNetwork Address Port Translation機能（以下「NAPT」と称す。）を搭載するルータによりローカルエリアネットワーク（以下「LAN」と称す。）とインターネットを接続することが一般化している。

【0003】インターネットに接続された機器間で通信を行なう場合、世界中で一意に割り当てられたグローバルIPアドレスが使用される。一方で、インターネットに接続される機器数の急増によりグローバルIPアドレスは不足する傾向にある。そのため、インターネットに直接接続されない組織内や家庭内のLANにおいては、RFC1918で規定されたLAN内でのみ一意なプライベートIPアドレスが使用されることが多い。プライベートIPアドレスはインターネット上において一意的なアドレスでないため、そのままではプライベートIP

アドレスを持つ機器はインターネットに接続された機器と通信を行うことができない。NATまたはNAPT機能はこの問題を解決し、プライベートIPアドレスを割り当てられた機器がインターネット経由で通信を行なえるよう、グローバルIPアドレスとプライベートIPアドレスの相互変換機能を提供する。

【0004】以下で、NAT機能の仕組みを図8の通信シーケンス図に沿って説明する。LAN711はルータ703を介してインターネット712に接続されている。機器701はLAN711に接続され、サーバ702はインターネット712に接続されている。機器701のIPアドレスはプライベートIPアドレス"192.168.1.2"であり、サーバ702のIPアドレスはグローバルIPアドレス"4.17.168.6"であるとする。ルータ703のインターネット側アドレスはグローバルIPアドレス"202.224.159.142"であるとする。ルータ703のインターネット側アドレスは説明の便宜上1つしかないとする。

【0005】上記ネットワーク構成において、機器701がサーバ702と通信を開始するためには、機器701は、まずIPパケット704をLAN711に送出する。IPパケット704には送受信先を特定するために、ソースIPアドレス（以下「SA」と称す。）、ディスティネーションIPアドレス（以下「DA」と称す。）、ソースポート（以下「SP」と称す。）、ディスティネーションポート（以下「DP」と称す。）を各々保存するフィールドと、任意の情報を運ぶためのペイロードとが含まれる。

【0006】次に、IPパケット704の宛先がグローバルIPアドレス"4.17.168.6"であることを検出したル

ータ703は、IPパケット704を往路変換708を行なってIPパケット705としてインターネット712に転送する。往路変換708においては、IPパケット704のSAフィールド内のプライベートIPアドレス"192.168.1.2"を、ルータ703のインターネット側のグローバルIPアドレス"202.224.159.142"に置換する。この際、ルータ703は、IPパケット704のSA"192.168.1.2"とIPパケット705のDA"4.17.168.6"の組を、図8（b）に示すようなルータ703内部に保持されるNATテーブル713に保存する。

【0007】変換708の結果、IPパケット705はグローバルIPアドレスのみを含んだ、インターネット上で転送が可能なパケットとなる。そのためIPパケット705は目的のサーバ702に転送され、サーバ702でパケット応答処理（S710）が行なわれ、応答のIPパケット706がルータ703に返信される。パケット応答処理（S710）においてパケットのSAとDAの値は交換される。

【0008】ルータ703はIPパケット706を受信すると、NATテーブル713との比較を行なう。比較により、IPパケット706のDAはIPアドレス705のSAと一致することから、ルータ703が送出したパケットに対する応答であることを確認し、その結果、復路変換709を行なう。

【0009】復路変換709において、ルータ703は、IPパケット706のDAフィールド内のグローバルIPアドレス"202.224.159.142"を、IPパケット706のSAフィールド内のIPアドレス"4.17.168.6"に基いてNATテーブル713に保存されていた機器701のIPアドレス"192.168.1.2"に置換し、IPパケット707としてLAN711へ転送する。これによりIPパケット707は機器701に送信され、機器701ではIPパケット704のレスポンスとして受信される。

【0010】NATテーブル713は通信を行なっている間保持され、通信が完了すると破棄される。通信完了の判定は通常、TCPパケットの場合はsynパケットの検出または通信が行なわれない時間によるタイムアウトにより行なわれ、UDPパケットではタイムアウトにより行なわれる。以上により、LAN上のサーバ702とインターネット上の機器701間で通信が可能となる。

【0011】以上の様に、NAT機能を持つルータにより、LAN上の機器とインターネット上の機器の通信が可能となる一方、NATの仕組みでは、LAN上の複数の機器が同時にインターネット上の機器と通信を行なうためには、同時に通信する機器と同じ数だけのグローバルIPアドレスをNATルータに割り当てる必要があり、グローバルIPアドレスの削減効果が小さくなる。この様な課題を解決するためにNATの機能を拡張した

NAPT機能がある。

【0012】以下で、NAPT機能の仕組みを図9の通信シーケンス図に沿って説明する。但し、図8のNATと同様の動作については説明を略する。NATではIPパケットのIPアドレスの変換のみを行なったが、NAPTにおいてはポートの変換も同時に行なう。すなわち、図9の往路変換808において、NATと同様の交換処理に加え、ルータ803が現在使用していないポート番号(ここでは「100」とする。)を選び、IPパケット804のSP(ここでは「1」とする。)の内容に置き換えてIPパケット805に変換する。この際、ルータ803は、IPパケット804のSA「192.168.1.2」とIPパケット805のDA「4.17.168.6」の組に加え、IPパケット804のSP(1)とそれを置換したルータ803のポート(100)の組をルータ803内部のNAPTテーブル813(図9(b)参照)に保存する。

【0013】ルータ803はIPパケット806を受信すると、受信パケットの内容とテーブル813との比較を行なう。比較した結果、受信したIPパケット806のDAがIPアドレス805のSAと一致し、IPパケット806のDPがIPアドレス805のSPと一致すれば、受信したパケット806がルータ803が送出したパケット805に対する応答であることを確認し、その結果、復路変換809を行なう。復路変換809においてはNATの動作に加え、IPパケット806のDP(ここでは「100」)の内容を保存してあったIPパケット804のSP(ここでは「1」)に置き換え、IPパケット807に変換する。これにより、LAN上の機器801とインターネット上のサーバ802間で通信が可能となる。上記のNAPT機能によれば、LAN側から複数の機器が同時に通信する場合でも、機器801からの通信をルータのポート番号により区別することができ、従ってルータ803のグローバルIPアドレスが1つだけであっても、ルータのポートの数だけ同時に通信を行なうことが可能となる。

【0014】以上の様に、NATまたはNAPT技術によれば、プライベートIPアドレスを持つLAN内の機器からインターネット上のサーバに接続することは容易に可能である。一方で、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望む時に自由に接続することが容易でなく、このため例えば、携帯電話からインターネット経由で、家庭内の家電機器に接続して制御するような機能の実現は難しかった。これは、LAN内の機器がプライベートIPアドレスを持つ上、インターネット上の機器からはプライベートIPアドレス宛てにパケットを送出することができないためである。この様な課題を解決するために例えば静的NATまたはポートフォワーディングと呼ばれる機能がある。

【0015】静的NAT機能においては、ユーザは予めルータに静的NATテーブルを設定する必要がある。静的NATテーブルのエントリは、接続したいLAN内の機器のIPアドレスとポート、及びルータの任意の空いているポートからなる。ユーザはインターネットからLAN内の機器に接続したい場合は、ユーザの端末から、ルータのグローバルIPアドレスと静的NATテーブルに設定されたポートの組を指定してパケット送信を行なう。ルータは、ユーザの端末から受信したパケットの内容を、予め設定してあった静的NATテーブルのエントリと照合して、パケットの送信先をエントリ内のLAN内の機器のIPアドレスとポートに置換して転送する。

【0016】

【発明が解決しようとする課題】以上の静的NATにより、インターネット上の機器からLAN内の機器に対し通信が可能になる。しかし、静的NATには、予めユーザが静的NATテーブルを設定しておく必要があり、その設定内容がIPアドレスの知識のないエンドユーザにとって複雑であるという問題があった。また、ルータのグローバルIPがPPPやDHCPプロトコルにより動的に割り振られている場合に、そのアドレスをユーザが把握することが難しく、接続先を特定できないという課題があった。さらに、外部からのパケットをLAN内に転送するためにセキュリティが低下すること、ユーザの管理するルータがISPのプライベートアドレスのネットワークに接続されている場合などNATが多段になっている場合にはISPのルータの静的NAT設定も行なわなければインターネットから通信が行なえないことなど、多くの課題があった。

【0017】以上説明した様に、プライベートIPアドレスを持つLAN内の機器からインターネット上の機器に接続することは容易だが、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望む時に自由に接続することが容易でなかった。このため例えば、PC(パーソナルコンピュータ)や携帯電話からインターネット経由で、家庭内のPCや家電機器に接続して制御するような機能の実現は難しかった。

【0018】本発明は上記の課題を解決することを目的とする。すなわち、本発明はプライベートIPアドレスを持つLAN内の機器に対しインターネット上の機器から望む時に自由に通信できる方法を提供する。特に、その場合に、ユーザがルータに対して事前に複雑な設定を行なっておく必要がなく、また、ルータのインターネット側アドレスが動的に割り振られている場合でも容易に通信先機器を指定でき、またNATルータが多段の場合でも、前述の通信を実現できる方法を提供する。

【0019】

【課題を解決するための手段】本発明に係る第1の通信システムは、インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1

つの端末との間の通信を、インターネットに接続されたサーバを介して転送する通信システムである。その通信システムにおいてサーバ及び機器は次のように動作する。

【0020】機器はサーバに定期的に通知パケットを送り、サーバは端末から機器に対する転送要求があった場合、通知パケットの応答として接続要求パケットを前記機器に送る。機器は、サーバから接続要求パケットを受信した場合、サーバに対してTCP接続要求を送信する。サーバは、接続要求パケットに応答して機器からサーバへ送信されたTCP接続要求を受諾し、これによりTCP接続を確立する。サーバは、TCP接続確立後、そのTCP接続上で端末と機器の間の通信を転送する。

【0021】第1の通信システムによれば、サーバから機器に送信される接続要求パケットは機器からの通知パケットの応答として送信されるため、機器がNAT機能を搭載したルータによってインターネットに接続されている場合でも、接続要求パケットを静的NAT設定無しにルータを越えて機器に届けることができる。またTCP接続の確立時に機器からサーバに対して接続要求が行われるため、やはり静的NAT設定を無しにTCP接続を確立することが出来る。これによりサーバと機器の間に何時でも望むときにTCP接続を確立することができ、このTCP接続上でサーバが通信の転送を行うことにより、端末からNATルータの有無に関わらず何時でも望む時にLANに接続された機器と通信を行うことが可能となる。さらに本発明は、通信の転送を行わない期間は負荷の軽いパケットを用い、通信の転送を行う期間は通信の信頼性が高いTCP接続を用いるため、サーバの負荷を軽くしながら信頼性有る通信を実現することができる。

【0022】本発明に係る第2の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。端末はサーバに対し機器IDを含んだHTTPリクエストを送信することにより機器に対する転送要求を行う。サーバは端末と機器の間の通信を転送する際に、端末からのHTTPリクエストを機器から張られたTCP接続上に転送する。機器は転送されたHTTPリクエストを処理して、それに対するHTTPレスポンスをTCP接続上でサーバへ応答する。サーバはHTTPレスポンスを端末へ転送する。第2の通信システムによれば、既存のWebブラウザを装備した端末から、NATルータの有無に関わらず何時でも望む時にLANに接続された機器とHTTPによる通信を行うことが可能となる。

【0023】上記の第2の通信システムにおいて、機器はWebサーバモジュールと転送モジュールを備えてもよい。Webサーバモジュールは、転送モジュールからHTTPリクエストを受信してHTTPレスポンスを返信する。転送モジュールは、サーバから接続要求パケットを受信した際はサーバに対してTCP接続要求を送信

してTCP接続を確立し、そのTCP接続上でサーバからHTTPリクエストを受信してWebサーバに転送し、WebサーバからHTTPレスポンスを受信してサーバにTCP接続上で転送する。

【0024】これによれば、既存のWebブラウザを装備した端末から、NATルータの有無に関わらず何時でも望む時にLANに接続された機器とHTTPによる通信を行うことが可能となるうえ、既存のWebサーバモジュールを機器に実装することができる。

10 【0025】本発明に係る第3の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。

【0026】サーバは、少なくとも1つの端末から複数の転送要求を受信することができ、端末から機器に対する複数の転送要求があった場合に、各々に一意なセッション識別子を生成し、接続要求パケットにより機器に通知する。機器は、サーバからセッション識別子を伴った接続要求パケットを受信した場合、サーバに対してTCP接続を確立し、その確立したTCP接続上でセッション識別子をサーバに送信し、TCP接続確立後は、TCP接続上でサーバと通信する。サーバは、接続要求パケットに

20 応答して機器からサーバへ送信されたTCP接続要求を受諾してTCP接続を確立し、TCP接続上で機器から送信されるセッション識別子を受信し、TCP接続に受信されたセッション識別子を対応付けることで、端末からの複数の接続要求に対して複数のTCP接続を各々対応付ける。サーバは、端末がセッション識別子を指定して接続を要求し、且つ、指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合、確立済みのTCP接続上で端末からの通信を転送することにより、セッション識別子毎に並列して通信内容の転送を行う。

【0027】第3の通信システムによれば、サーバと機器の間に複数のTCP接続を確立することができ、その際の個々のTCP接続上の通信内容を別々のセッションIDで管理することで、内容を混合して一貫性を無くすることなく、端末から機器に対しセッションID毎に並列した通信を行うことが可能となる。

【0028】第1の通信システムにおいてサーバは複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、次のように動作してもよい。サーバは、機器からの定期的な通知パケットを受信したときに、最終アクセス時刻を通知パケットの受信時刻で更新する。そして、端末から機器に対する転送要求があった際に、機器の最終アクセス時刻と現在時刻との差が所定値を超えた場合は、接続要求を拒否する。その差が所定値以下の場合は、通知パケットの応答として接続要求パケットを前記機器に送る。

【0029】これによれば、機器が動作して通信可能なことが端末からサーバに接続要求があった際に直ちに確

認できるため、通信不可能な場合に端末に対する拒否の応答が高速に出来、また機器のIPアドレスがISPによって動的に割り当てられており、かつ機器の電源断などにより、サーバに登録された機器のIPアドレスが既に関係無い別の機器に割り当てられた場合でも、誤って関係の無い別の機器に接続要求を行うことを回避できる。

【0030】本発明に係る第4の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。

【0031】サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備える。サーバは、機器に予め最大アクセス確認周期情報を送信する。機器は、その最大アクセス確認周期情報を受信して内部に保存しておき、最大アクセス確認周期情報が示す周期よりも短い周期で定期的に通知パケットを送信する。サーバは、機器から通知パケットを受信した際に最終アクセス時刻を通知パケットの受信時刻で更新する。サーバは、端末から機器に対する転送要求があった際に、機器の最終アクセス時刻と現在時刻との差が最大アクセス確認周期情報が示す周期を超えている場合は接続要求を拒否し、その差が最大アクセス確認周期情報が示す周期以下の場合は、通知パケットの応答として接続要求パケットを前記機器に送信する。

【0032】第4の通信システムによれば、機器が動作して通信可能なことが端末からサーバに接続要求があった際に直ちに確認できるため、通信不可能な場合に端末に対する拒否の応答が高速に出来、また機器のIPアドレスがISPによって動的に割り当てられており、かつ機器の電源断などにより、サーバに登録された機器のIPアドレスが既に関係無い別の機器に割り当てられた場合でも、誤って関係の無い別の機器に接続要求を行うことを回避できる。さらに、サーバから機器に予め最大アクセス確認周期情報を指定することで機器が通信可能な状態であることを確認する通知パケットの送信周期を制御し、サーバにおいて通知パケットの受信負荷と通信不可能なことを検出するまでの時間をトレードオフによって自由に調整することが可能となる。

【0033】本発明に係る第5の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。

【0034】サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備える。端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段とを備える。機器は、通信を暗号化および復号化する暗号通信手段を備える。サーバは、端末と機器の間で秘密情報を転送する際、予め端末にサーバ証明書を送信する。端末は、サーバと秘密情報の送受信を、サーバ証明書を認証して正規であることを確認した後に暗号通信手段により暗号化して行う。機器

は、サーバと秘密情報の送受信を、確立されたTCP接続で暗号通信手段により暗号化して行う。サーバは、確立されたTCP接続を介して端末から機器へ秘密情報を転送する際は、端末から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して機器に送信する。または、機器により確立されたTCP接続を介して機器から端末へ秘密情報を転送する際は、機器から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して前記端末に送信する。

【0035】第5の通信システムによれば、端末と機器の間で秘密に通信を行うことが出来、さらに端末から接続先を認証するためのサーバ証明書が各機器に不要でサーバに1種類で良いなど特に効果がある。

【0036】本発明に係る第6の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。

【0037】サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備える。端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備える。機器は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備える。サーバは、端末と機器の間で秘密情報を転送する際、予め前記端末と前記機器に各々サーバ証明書を送信する。端末は、サーバと秘密情報の送受信を、サーバ証明書を認証して正規であることを確認した後に暗号通信手段により暗号化して行う。機器は、サーバと秘密情報の送受信を、サーバ証明書を認証して正規であることを確認した後に機器が確立したTCP接続上で暗号通信手段により暗号化して行う。サーバは、機器により確立されたTCP接続を介して端末から機器へ秘密情報を転送する際は、端末から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して機器に送信する。又は、機器により確立されたTCP接続を介して機器から端末へ秘密情報を転送する際は、機器から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して前記端末に送信する。

【0038】第6の通信システムによれば、端末と機器の間で秘密に通信を行うことができ、さらに端末から接続先を認証するためのサーバ証明書が各機器に不要でサーバに1種類で良く、かつ機器から接続先を認証するためのサーバ証明書も各機器に不要でサーバに1種類で良いなど特に効果がある。

【0039】本発明に係る第7の通信システムは、インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を、インターネットに接続されたサーバが転送する通信システムである。その通信システムにおいてサーバ等は次のように動作する。

【0040】サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備える。機器は、サーバに第1及び第2の通知パケットを定期的に送り、第1の通知パケットの送信周期は第2の通知パケットの送信周期よりも長い。サーバは、機器から第1及び第2の通知パケットを受信し、機器から第1の通知パケットを受信したときに最終アクセス時刻を受信時刻で更新し、第2の通知パケットを受信したときには最終アクセス時刻を更新しない。サーバは、端末から機器に対する転送要求があった際に、機器の最終アクセス時刻と現在時刻との差が所定期間を超えている場合は接続要求を拒否し、その差が所定期間以下の場合は、第1及び第2の通知パケットの応答として接続要求パケットを前記機器に送る。機器は、サーバから接続要求パケットを受信した場合、サーバに対してTCP接続要求を送信する。サーバは、接続要求パケットに応答して機器からサーバへ送信されたTCP接続要求を受諾し、これによりTCP接続を確立する。サーバは、TCP接続が確立後、そのTCP接続上で端末と機器間の通信を転送する。

【0041】第7の通信システムによれば、機器が動作して通信可能なことが端末からサーバに接続要求があった際に直ちに確認できるため、通信不可能な場合に端末に対する拒否の応答が高速に出来、また機器のIPアドレスがISPによって動的に割り当てられており、かつ機器の電源断などにより、サーバに登録された機器のIPアドレスが既に関係無い別の機器に割り当てられた場合でも、誤って関係の無い別の機器に接続要求を行うことを回避できる。さらに本発明によれば、通知パケットを第1および第2の通知パケットの2種類に区別し、最終アクセス時間更新を第1の通知パケット受信時に限ることで、NATルータが接続要求パケットを通知パケットの応答とみなす時間が短いために通知パケットの送信頻度を高くしなければならない場合でも、サーバにとって負荷の高い最終アクセス時間更新の頻度を高くしなくても良い効果がある。

【0042】上記の通信システムにおけるサーバ、機器の機能は、コンピュータのようなプログラム可能な装置で所定のプログラムを実行させることにより実現されてもよい。そのプログラムはコンピュータ読み取り可能な記録媒体により提供されてもよい。

【0043】

【発明の実施の形態】以下、添付の図面を参照し、本発明に係る通信システムの実施の形態を詳細に説明する。

【0044】（実施の形態1）図1は本発明の実施の形態1の通信システムの通信シーケンスを説明した図である。図2は本発明の通信システムのネットワーク接続図である。本発明の通信システムはローカルエリアネットワーク（LAN）106上の機器とインターネット105上の機器間の通信を実現するものであり、LAN106に接続された機器101と、インターネット105上

に接続されたサーバ104と、LAN106とインターネットを接続するルータ103を含む。インターネット105には通信端末102も接続されている。

【0045】ルータ103はNAPT機能を実装している。機器101のIPアドレスはプライベートIPアドレス"192.168.1.2"であり、サーバ104のIPアドレスはグローバルIPアドレス"4.17.168.6"であるとする。ルータ103のインターネット105側アドレスは一般にインターネットサービスプロバイダからDHCPやPPP等のプロトコルにより割り当てられ、動的に変化するが、この時点でルータ103のインターネット側アドレスはグローバルIPアドレス"202.224.159.142"であるとする。説明の便宜上、ルータ103のインターネット105側アドレスは1つしかないとする。なお、本実施の形態において、IPアドレスはIPv4に準拠している。

【0046】図1を参照し、本実施形態の通信シーケンスを説明する。機器101はまず、サーバ104に対し最大アクセス確認周期情報要求107を送信する。サーバはこの応答として、最大アクセス確認周期情報通知108を送信する。これらの通信107、108はUDPによってもTCPによっても良く、LAN106側に接続された機器101から開始されるため、NAPT機能を備えたルータ103を越えて支障なく通信できる。ここで、最大アクセス確認周期とは、機器101からサーバ104へ送信される通知UDPパケット（後述）の送信時間間隔の最大値を示すものであり、例えば「5分」というような値となる。

【0047】次に、機器101は周期的に通知UDPパケット109を送信する。この周期は先に取得した最大アクセス確認周期の値（例えば5分）より小さい間隔で送られる。通知UDPパケット109は機器101に固有に付与された機器識別子である「機器ID」を含む。通知UDPパケット109はルータ103により、往路のNAPT変換が行なわれた後インターネット105に送出され、サーバ104にて受信される。

【0048】図3の（a）、（b）に各々変換される前後の通知UDPパケットの内容を示す。通知UDPパケットの送信周期は、ルータ103がUDPパケットのNAPTテーブルをタイムアウトにより破棄する時間よりも短く設定する。これによりルータ103には、図9（b）に示したようなNAPTテーブルがタイムアウトせず継続的に保持される。

【0049】図1に戻り、サーバ104は、通知UDPパケット109を受信すると、ヘッダ内のSA、DA、SP、DPの各アドレスと機器IDを取り出し、図4に示すように、これらの情報を機器101（機器ID="1234"）に対応する1組のエントリとしてサーバ内に登録保存する（ステップS119）。また、ステップS119では、最終アクセス時刻をエントリに付加し、

19

サーバ104が通知UDPパケット109を受信した時刻を記録する。以後、サーバ104は、通知UDPパケット109を受信するたびにステップS120に示すように機器に対応するエントリの最終アクセス時刻を更新する。また、この際、通知UDPパケット109のヘッダ内のSA、SPの各アドレスが変更されていた場合は、エントリ中のそれらのアドレスの値も更新する。これにより、ルータ103のインターネット(WAN)105側IPアドレスが動的に割り振られていても、最新のアドレスがエントリに保持される。以上のシーケンス

10 10の実行により、通信の準備が完了する。
【0050】以上の通信準備が完了している状況で、端末102から機器101に対する通信を開始したい場合、端末102は機器101の機器IDをパラメータに指定して、サーバ104に対し機器接続要求110を送信する。なお、機器IDは端末102が予め認識しているものとする。機器接続要求110を受信したサーバ104は、端末102により指定された機器IDを検索キーとして図4に示すテーブルからサーバ内に登録された機器IDを検索し、機器101が登録した対応エントリ

20 20を得る(ステップS121)。
【0051】次に、サーバ104はエントリ内の最終アクセス時刻を確認し、現在時刻との差が最大アクセス確認周期を超えている場合は機器接続要求110を拒否し、最大アクセス確認周期以下の場合は、ステップS122以後に進んで機器101に接続要求UDPパケット111を送信する。

【0052】このように最終アクセス時刻を確認することで、機器101が正常に動作し、かつ、ごく最近まで正常に通信できていたか否かが直ちに確認できるため、機器接続要求110の受諾可否判定が高速にできる。また、ルータ103のインターネット(WAN)105側IPアドレスはISPによって動的に割り当てられているため、機器101の電源遮断後ある程度時間が経過すると、サーバ104に登録された機器101のIPアドレスが別の機器に割り当てられてしまう場合があるが、この場合でも誤って関係の無い別の機器に接続要求を行うことを防止できる。

【0053】次に、サーバ104は、一意なセッション識別子を生成してサーバ内に保存する(ステップS122)。さらに、サーバ104は機器101に対応するエントリからSA、DA、SP、DPの各アドレスを取得し、これらを用いてセッション識別子をペイロードに含む接続要求UDPパケット111を送信する。ここで、接続要求UDPパケット111は通知UDPパケット109に対する応答として構成されている。図3(c)にインターネット(WAN)105上に送出された接続要求UDPパケットの内容を示す。図3(c)に示すパケットのアドレスとポートの値は、それぞれ図3(b)に示すパケットにおいてアドレスとポートのソースとディ

20

スティネーションの値を入れ替えた値となっている。これにより、接続要求UDPパケット111は通知UDPパケット109の応答パケットであることが分かる。接続要求UDPパケット111は、ルータ103において復路のNAPT変換により図3(c)に示す構成から図3(d)に示す構成に変換され、機器101に転送される。

【0054】接続要求UDPパケット111を受信した機器101は、サーバ104に対してTCP接続要求112を送信する。TCP接続要求112についての詳細な説明は省略するが、syn, ack/syn, ackパケットによって接続を確立する通常のTCP接続確立手順である。TCP接続要求112はLAN側からWAN側に対して行なわれるものであるため、NAPT機能を備えたルータ103を越えて支障なくTCP接続を確立することができる。

【0055】以上によりサーバ104と機器101の間でTCP接続が確立されたが、UDPパケットはコネクションレス型であるため、そのままではサーバ104において、TCP接続が接続要求UDPパケット111に応じて確立されたか否かの判定ができない。そのために以下で説明する手順が実行される。

【0056】まず、機器101はそのTCP接続上で、接続要求UDPパケット111により通知されたセッション識別子を、セッション識別子通知113によってサーバへ返送する。サーバ104はセッション識別子を受信すると、ステップS123においてセッション識別子の照合を行う。照合の結果、このセッション識別子が機器接続要求110により生成されたものであることを検出すると、サーバ104はこのTCP接続を、接続要求110に答えて端末102と機器101間の通信の転送に使用することを決定する。

【0057】なお、セッション識別子に代えて機器IDを用いてもTCP接続と接続要求UDPパケットを対応付けることはできるが、その場合はサーバ104と機器101の間には同時に複数のTCP接続を確立することができないという問題が生じる。本実施の形態によれば、サーバ104と機器101の間に複数のTCP接続を確立することができ、その際の個々のTCP接続上の通信内容を別々のセッション識別子で管理することで、複数の通信の内容を無秩序に混合してしまうことなく、別々のTCP接続上で各々一貫性を保持した通信の転送を行ない、端末102から機器101に対しセッション識別子毎に並列して複数の通信を行うことが可能となる。

【0058】以上述べた手順により、サーバ104と機器101の間でTCP接続が確立されると、サーバ104はそのTCP接続上で端末102と機器101間の通信の転送を開始する。すなわち、サーバ104は端末102からの通信114を通信115として機器101に

転送し、機器101からの通信116を端末102に通信117として転送する。最後に、通信が完了すると、サーバ104または機器101からTCP切断118を行い、通常のTCP接続の切断を行なって一連のシーケンスが完了する。

【0059】なお、上記のサーバ104による通信の転送は、TCP接続が維持されている間は何度でも繰り返して行なうことが可能であり、これにより端末102と機器101の間で一連の通信を行なうことができる。また、図1では端末104からの通信に対し機器101が10 応答する様子を図示しているが、これに限らず、どのような手順のプロトコルの通信の転送をもTCP接続が維持されている間に行なうことが可能である。

【0060】以上説明したように本実施の形態によれば、通知UDPパケット109への応答として接続要求UDPパケット111を送ることで、プライベートIPアドレスを持つLAN内の機器101に対し、インターネット上の端末102から所望のタイミングで自由に通信を開始できる。これにより、例えば、端末としてインターネットに接続された携帯電話やPDAを用い、機器20 としてLANに接続された、ビデオ、テレビ、エアコン、冷蔵庫などの家電を用いれば宅外から自由に家電操作を行なうことも可能となる。

【0061】また、本実施の形態によれば、ルータ103は通常のNAPT動作のみを行なえばよく、静的NAT、静的NAPT設定等が不要なため、事前にユーザがルータに対して複雑な設定を行なう必要が無い。

【0062】また、本実施の形態によれば、ルータ103に静的NATを設定せず、機器101に対してWAN側から到達可能なパケットが、機器101が通知UDP30 パケットを送信している期間にサーバ104から送信されるパケットに限定される。これにより、第3者からの攻撃を受けにくく、セキュリティが向上する。

【0063】また、本実施の形態によれば、LAN内からインターネットに対して周期的に通知UDPパケット109が送信される。これにより、このパケットがルータ103に対し、いわゆるキープアライブパケットとして作用し、ルータ103のWAN側接続のPPPやDHCPがタイムアウトすることによってISPから切断されてしまうことを防ぎ、いつでもインターネットから通信40 可能な状態に維持するという効果を持つ。

【0064】また、本実施の形態によれば、サーバ104から最大アクセス確認周期情報通知108によって通知UDPパケット109の送信周期の長短を変更することで、サーバにおける通知UDPパケット109の受信負荷と通信不可能なことを検出するまでの時間を、互いにトレードオフして自由に調整することが可能となる。

【0065】また、本実施の形態によれば、ルータ103のWAN側IPアドレスが動的に割り振られていても、通知UDPパケット109により周期的に最新のW50

AN側IPアドレスがサーバ104に登録されるため、端末102からは機器IDを指定するのみで容易に機器101を指定して通信ができる。

【0066】また、本実施の形態において、負荷の低いUDP通信により通信の準備を行ない、端末102と機器101との通信自体はデータロスにくく信頼性の高いTCP通信を行なうことが好ましい。これにより、サーバ104の負荷の低さと、端末102と機器101との通信の信頼性を両立することができる。通信を準備する通知UDPパケット109は、ルータ103のNAPTテーブルのタイムアウト以下の間隔で送出する必要があり、送信頻度が高くなるため、UDPパケットとすることによる負荷削減効果が大きく、一方で周期的に送信されるために多少のパケットロスがあっても次の送信で復帰するために影響が小さいなど、UDPパケットを使用する事に特に利点がある。

【0067】なお、本実施の形態ではNAPTによって説明したが、ルータ103がNAT動作を行なっている場合であっても、機器101とサーバ104の動作を変更することなしに、図1のシーケンスが支障無く動作する。また、本実施の形態において、ユーザがNAT機能を有するルータを用いず、機器101を直接インターネット105に接続している場合であっても、機器101とサーバ104の動作を変更することなしに、図1のシーケンスが可能となる。さらに、本実施の形態において、ユーザがプライベートIPアドレスを使用するISPに加入し、その結果、ユーザのルータとISPのルータをあわせて多段のNATルータを介してインターネットによって接続されている場合でも、その各々の段のルータにおいて通常のNATまたはNAPT動作が行なわれ、やはり機器101とサーバ104の動作を変更することなしに、図1のシーケンスが支障無く動作する。

【0068】なお、アドレス登録は通知UDPパケットに必須の機能ではなく、他の手段によってアドレス登録を行なっても本発明の効果は失われないが、周期的な送信が必要な、グローバルIPアドレスを登録するパケットとNATテーブルを維持するパケットの2種類を兼用するため効率が良く、特に好適な構成である。

【0069】なお、セッション識別子はTCP接続要求112に対しTCP接続を一意に対応付けられる範囲で一意であれば良く、例えばサーバ内で一意でなくとも、機器IDと組み合わせた場合に一意であっても良い。

【0070】なお、本実施の形態ではIPv4のアドレスを例示して説明したが、IPv6のアドレスを用いた場合でも、LAN内からインターネットへのパケットとそのパケットに対する応答は透過するが、インターネットからLAN内へのパケットは透過しないルータやゲートウェイを採用する限りにおいて本発明は同じ効果を有する。

【0071】なお、本実施の形態では端末102はイン

ターネットに直接接続されるように図示されているが、端末102がLANに接続されていても端末102から通信を開始する限りにおいてサーバ104に対する通信に支障はないため、本発明の効果は同様に発揮される。さらに、端末102に機器101と同様の機能を搭載すれば、端末102と機器101がともにLAN内にあっても互いに通信を開始することが出来る構成となり、完全に対称な通信システムを構成できることは明らかである。

【0072】なお、本実施の形態では機器101からの接続先はサーバ104のみであり、サーバ104が端末102と機器101間の通信を転送したが、接続要求UDPパケット111により端末102のアドレスを通知すれば、機器101が端末102に対し直接TCP接続要求112を送信する構成も可能である。この構成によれば、端末102と機器101が直接通信を行なうことが可能になり、サーバ104の転送負荷が低減されるなど別の効果がある。

【0073】なお、本実施の形態においてサーバは端末と機器の通信の転送のみを行ったが、同時にサーバ自身がTCP接続を用いて機器と通信を行うことも可能である。このような構成によればサーバは端末に対して機器への通信機能を提供すると同時に、機器の設定や監視、ソフトウェアのアップデートを行うなど機器へのサービスを提供することも可能である。

【0074】なお、本実施の形態において機器101およびサーバ104をコンピュータで構成することができる。その際に、機器101とサーバ104に各々図1のシーケンスを実行させるコンピュータプログラムを作成することが可能であり、またそれらを各々媒体に蓄積し配布することができる。これによれば汎用のコンピュータを用いて宅外からの通信を実現することができる。

【0075】(実施の形態2) 本発明に係る通信システムの別の実施形態を説明する。本実施形態のネットワーク接続は図2で示したとおりである。アドレス付与も第1の実施の形態と同じであり、通信シーケンスのみが異なっている。本実施の形態では端末としてWebブラウザを備えたPCや携帯電話を用いており、これを用いてLANに接続された機器101とHTTPによる通信を行なって操作やコンテンツ取得などを行なうものである。

【0076】図5を参照し、本実施形態の通信シーケンスを説明する。機器101はまず、サーバ104に対し最大アクセス確認周期情報要求407を送信する。サーバ104はこの応答として、最大アクセス確認周期情報通知408を送信し、最大アクセス確認周期の値(例えば5分)を通知する。この通信はUDPによってもTCPによってもよく、LAN106側に接続された機器101から開始されるため、NAPT機能を備えたルータ103を越えて支障なく通信できる。

【0077】次に、機器101は2種類の通知UDPパケットA、B(410、409)を各々周期的に送信する。2種類のパケットA、Bの差異は、通知UDPパケットAが最終アクセス時間を更新する機能を持っているのに対し、通知UDPパケットBは最終アクセス時間を更新する機能を持たないことである。その他の点については同じである。

【0078】機器101から通知UDPパケットA(410)を送信する周期は先に取得した最大アクセス確認周期の値(例えば5分)より小さい間隔で送られる。一方、通知UDPパケットAまたはBのいずれかを送信する周期はルータ103がUDPパケットのNAPTテーブルをタイムアウトにより破棄する時間よりも短く設定する。

【0079】実施の形態の1においては通知UDPパケットは1種類しかなかったため、その送信周期は前記の条件のうち周期の短いほうにあわせて設定する必要があった。そのため、ルータ103のNAPTテーブルの破棄時間が短い(例えば30秒)の場合、通知UDPパケットが30秒周期以下の高頻度で送信され、その度ごとに最終アクセス時刻が更新されるため、ルータ103のWAN側のアドレス変更が無い場合でもエントリの更新作業が行なわれ、サーバ負荷が増大するという問題があった。本実施の形態は、最終アクセス時刻の更新周期を、ルータ103のNAPTテーブルの破棄時間と関係なく独立に設定することができ、負荷を削減しやすいという効果を有する。

【0080】通知UDPパケットA、Bは機器101に固有に付与された機器識別子である機器IDを含む。通知UDPパケットA、Bは、ルータ103により往路のNAPT変換が施されてインターネットに送出され、サーバ104で受信される。NAPT変換の内容は実施の形態の1と同様である。また、通知UDPパケットによりルータ103内のNAPTテーブルがタイムアウトせず継続的に保持される点も同じであり、サーバ104内のエントリに、機器101にパケットを送信するためのアドレスが登録される点(ステップS421)、エントリ中の最新アクセス時刻の更新(ステップS422)についても実施の形態の1と同様である。ここまでのシーケンスの実行により、通信の準備が完了する。

【0081】以上の通信準備が完了している状態で、端末102から機器101に対する通信を開始する場合、端末102はサーバ104に対し、「GET connect.cgi?ID=1234」のように機器101の機器IDをパラメータに指定して、HTTPリクエストとして機器接続要求411を送信する。なお、機器ID"1234"は端末102が予め認識しているものとする。機器接続要求411を受信したサーバ104は、ステップS423において、指定された機器IDをキーにサーバ内に登録された機器IDを検索し、機器101が登録した対応エントリを得

る。

【0082】次に、サーバ104はエントリ内の最終アクセス時刻(図4参照)を確認し、それと現在時刻との差が最大アクセス確認周期を超えている場合は機器接続要求411を拒否し、最大アクセス確認周期以内の場合は、ステップS424以後に進んで機器101に接続要求UDPパケット412を送信する。この最終アクセス時刻の確認により、第1の実施の形態と同様に、誤って関係の無い別の機器に接続要求を行うことを回避できる等の効果がある。

【0083】次にサーバ104は、ステップS424において一意なセッション識別子を生成してサーバ104内に保存する。さらに、サーバ104は機器101に対応するエントリからSA、DA、SP、DPの各アドレスを取得し、これらを用いてセッション識別子をペイロードに含む接続要求UDPパケット412を送信する。ここで、接続要求UDPパケット412は通知UDPパケットA(410)または通知UDPパケットB(409)に対する応答として構成されているため、ルータ103において、復路のNAPT変換が行なわれて機器101に転送される。

【0084】接続要求UDPパケット412を受信した機器101は、サーバ104に対してTCP接続要求413を送信する。TCP接続要求413についての詳細な説明は省略するが、syn, ack/syn, ackパケットによって接続を確立する通常のTCP接続確立手順である。TCP接続要求413はLAN側からWAN側に対して行なわれるものであるため、NAPT機能を備えたルータ103を越えて支障なくTCP接続を確立することができる。

【0085】以上によりサーバ104と機器101の間でTCP接続が確立された後、機器101はそのTCP接続上で、接続要求UDPパケット412により通知されたセッション識別子を、セッション識別子通知414によってサーバ104へ返送する。サーバ104はセッション識別子を受信すると、ステップS425でセッション識別子の照合を行い、このセッション識別子が機器接続要求411により生成されたものであり、従って機器接続要求411に対するTCP接続確立が成功したことを検出する。

【0086】その後、サーバ104はHTTPリクエスト411に対する応答としてHTTPレスポンス415を端末102に送信する。このHTTPレスポンス415は、端末102に表示すべきHTMLコンテンツを含んでおり、かつ、このHTMLコンテンツにはセッション識別子"5678"が、例えば「リンク」のようにリンクやボタンとして埋め込まれている。以上の手順により、端末102には機器101に対応するページ(画像)が表示される。

【0087】次に、ユーザが表示されたページ内のリンクをクリックすると、"GET control.cgi?SessionID=5678&Target=deviceFunc.cgi&Param=abcd"等のようにセッション識別子を含むHTTPリクエスト416が生成されてサーバ104に送信される。サーバ104はHTTPリクエスト416を受信すると、指定されたcontrol.cgiが起動し、セッション識別子"5678"を照合する(ステップS426)。照合した結果、セッション識別子"5678"のTCP接続が既に確立済みであることを検出すると、サーバ104のcontrol.cgiは、HTTPリクエスト416の内容を"GET deviceFunc.cgi?Param=abcd"のように変換してHTTPリクエスト転送417としてそのTCP接続上に転送する。このようにして、端末102は、機器101に対するHTTPリクエストを送信できる。

【0088】本発明の端末と機器間の通信転送において、上記で説明したような変換方式を用いると、端末は従来のWebブラウザをなんら変更することなく動作可能な上、機器上の"deviceFunc.cgi"等の所望のcgiと"Param=abcd"等の所望のパラメータを指定して起動させるHTML文書を機器が自由に記述することが可能になるなど、優れた効果を持つ。

【0089】HTTPリクエスト転送417を受信した機器101は、その応答としてHTTPレスポンス418を返信する。この動作について図6を用いて詳細に説明する。

【0090】図6に示すように、機器101は転送モジュール501とWebサーバモジュール502を備える。転送モジュール501はサーバ104との間で本発明の通信プロトコルによる通信を行なうためのモジュールであり、Webサーバモジュール502は通常のWebサーバである。転送モジュール501は前述の様に、接続要求UDPパケット412を受信してTCP接続要求413を行い、HTTPリクエスト転送417を受信する。この際の転送モジュール501の通信方向に注目すると、TCP接続を要求(413)する一方でHTTPリクエスト(417)を受信しており、クライアントからTCP接続を要求され且つHTTPリクエストを受信する通常のWebサーバとは通信の方向が異なる。本実施の形態では、転送モジュール501がこの方向の違いを吸収し、Webサーバモジュール502に対し、ソケット等を通じて内部的にHTTPリクエスト503の送信、HTTPレスポンス504の受信を行なうことで、通常のWebサーバを用いて、本発明のHTTP通信手順が実装できるという効果を有する。

【0091】図5に戻り、次に、サーバ104により、HTTPレスポンス418がHTTPレスポンス転送419として端末102に返送される。HTTPレスポンス転送419に含まれるHTMLコンテンツには、セッション識別子がリンクやボタンとして埋め込まれてお

り、手順416～419と同様の手順を繰り返すことにより、端末102から機器101に対して継続的にHTTTPによるアクセスを行なうことが可能になる。この通信のHTMLコンテンツ生成は機器101で行なわれ、コンテンツ表示と操作は端末102で行なわれることにより、端末102から機器101を自由に操作したり、コンテンツを取得したりできる。

【0092】最後に、通信が完了すると、サーバ104または機器101がTCP切断420を行い、TCP接続の切断を行なって一連のシーケンスが完了する。

【0093】以上説明したように本実施の形態によれば、第1の実施の形態同様、プライベートIPアドレスを持つLAN内の機器101に対し、インターネット上の端末102から任意のタイミングで自由に通信を開始できる。これにより、端末としてWebブラウザを搭載したPCや携帯電話により、家庭内の機器を自由に操作したり、コンテンツを取得することができる。

【0094】また、第1の実施の形態同様、ルータ103は通常のNAPT動作のみを行なえばよく、静的NAT/NAPT設定等が不要なため、事前にユーザがルータに対して複雑な設定を行なう必要が無い。

【0095】また、第1の実施の形態同様、第3者からの攻撃を受けにくく、セキュリティが向上するという効果を有する。

【0096】また、第1の実施の形態同様、ルータ103のWAN側接続のPPPやDHCPがタイムアウトすることによってISPから切断されてしまうことを防ぎ、いつでもインターネットから通信可能な状態に維持するという効果を奏する。

【0097】また、第1の実施の形態同様、サーバ104における通知UDPパケットA410の受信負荷と通信不可能なことを検出するまでの時間を、互いにトレードオフして自由に調整することが可能となる。

【0098】さらに、最終アクセス時刻を更新する機能を持つパケットと持たないパケットの2種類の通知UDPパケットを用意することで、上記の時間の調整を、ルータ103のNAPTテーブルの破棄時間と関係なく独立に行なうことができるという効果を有する。

【0099】また、第1の実施の形態同様、端末102からは機器IDを指定するのみで容易に機器101を指定して通信ができる。

【0100】また、第1の実施の形態同様、UDPパケットによるサーバ104の負荷の低さと、TCPパケットによる端末102と機器101との通信の信頼性を両立することができる。

【0101】また、本実施の形態によれば、端末102に通常のWebブラウザを搭載した端末を用い、機器101に通常のWebサーバを搭載してHTTPの応答を実装することができるため、汎用性が高く、ユーザの使い勝手のよい通信システムを低コストに構成できる。

【0102】なお、本実施の形態ではNAPTによって説明したが、ルータ103がNATを行なっている場合であっても、機器101とサーバ104の動作を変更することなしに、図5に示す通信シーケンスを支障無く実現できる。また、本実施の形態において、ユーザがNATルータを用いず、機器101を直接インターネット105に接続している場合であっても、機器101とサーバ104の動作を変更することなしに、図5のシーケンスが支障無く実現できる。さらに、本実施の形態において、ユーザがプライベートIPアドレスを使用するISPに加入し、その結果、ユーザのルータとISPのルータをあわせて多段のNATルータを介してインターネットによって接続されている場合でも、その各々の段のルータにおいて通常のNATまたはNAPT動作が行なわれ、やはり機器101とサーバ104の動作を変更することなしに、図5のシーケンスを支障無く実現できる。

【0103】なお、アドレス登録は通知UDPパケットに必須の機能ではなく、他の手段によってアドレス登録を行なっても本発明の効果は失われないが、周期的な送信が必要な、グローバルIPアドレスを登録するパケットとNATテーブルを維持するパケットの2種類を兼用するため効率が良く、特に好適な構成である。

【0104】なお、セッション識別子はHTTPリクエスト411に対しTCP接続を一意に対応付けられる範囲で一意であれば良く、例えばサーバ内で一意でなくとも、機器IDと組み合わせた場合に一意であっても良い。

【0105】また、IPアドレスにIPv6のアドレスを用いてもよい。この場合、LAN内からインターネットへのパケットとそのパケットに対する応答は透過するが、インターネットからLAN内へのパケットは透過しないルータやゲートウェイを採用する限りにおいて本発明は同じ効果を有する。

【0106】なお、本実施の形態では端末102はインターネットに直接接続されるように図示されているが、端末102がLANに接続されていても端末102から通信を開始する限りにおいてサーバ104に対する通信に支障はないため、本発明の効果は同様に発揮される。さらに、端末102に機器101と同様の機能を搭載すれば、端末102と機器101がともにLAN内にあっても互いに通信を開始することが出来る構成となり、完全に対称な通信システムを構成できることは明らかである。

【0107】なお、本実施の形態では機器101からの接続先はサーバ104のみであり、サーバ104が端末102と機器101間の通信を転送したが、接続要求UDPパケット412により端末102のアドレスを通知すれば、機器101が端末102に対し直接TCP接続要求413を送信する構成も可能である。この構成に拠れば、端末102と機器101が直接通信を行なうこと

が可能になり、サーバ104の転送負荷が低減されるなど別の効果がある。

【0108】なお、本実施の形態においてサーバは端末と機器の通信の転送のみを行ったが、同時にサーバ自身がTCP接続を用いて機器と通信を行うことも可能である。このような構成によればサーバは端末に対して機器への通信機能を提供すると同時に、機器の設定や監視、ソフトウェアのアップデートを行うなど機器へのサービスを提供することも可能である。

【0109】なお、本実施の形態において機器101およびサーバ104をコンピュータで構成することができる。その際に、機器101とサーバ104に各々図4のシーケンスを実行させるコンピュータプログラムを作成することが可能であり、またそれらを各々媒体に蓄積し配布することができる。これによれば汎用のコンピュータを用いて家庭外からの通信を実現することができる。

【0110】（実施の形態3）本発明の通信システムの第3の実施の形態を説明する。本実施の形態のネットワーク接続は図2で示されたとおりである。アドレス付与も前述の実施の形態と同じであり、通信シーケンスのみが異なっている。本実施の形態では端末としてWebブラウザを備えたPCや携帯電話を用いており、これを用いてLANに接続された機器101とHTTPによる通信を行なって操作やコンテンツ取得などを行なう。

【0111】図7を参照して、本実施の形態の通信シーケンスを説明する。本実施の形態の通信シーケンスは、通知UDPパケットによって通信準備が行なわれるまでの手順は、図5で示した実施の形態2のシーケンスと同じである。図7にはそれ以降の手順を図示している。

【0112】端末102から機器101に対する通信を開始したい場合、端末102はサーバ104に対し、SSLでのTCP接続要求607を送信する。これにより通常のSSLの手順に従ってサーバ証明書通知608がサーバ104から端末102に送付されて、ステップS624で認証される。認証が成功すると暗号化通信が可能となる。続いて、第2の実施の形態と同じ手順に従って、機器接続要求609からTCP接続要求611までのシーケンスが実行される。

【0113】第2の実施の形態と異なる第1の点は、機器接続要求609が暗号化されていることである。これにより機器接続要求609に含まれる機器IDを秘匿する点ができる。また、第2の異なる点は、ステップS626において乱数が生成されてサーバ内に保存され、さらに接続要求UDPパケット610により機器に通知される点である。

【0114】次に、機器101がTCP/SSL接続要求611を送信し、サーバ104との間でTCP接続を接続する。これにより通常のSSLの手順に従ってサーバ証明書通知612がサーバ104から機器101に送付されて、認証される（ステップS627）。認証が成

功すると暗号化通信が可能となる。

【0115】以上によりサーバ104と機器101の間でSSLで暗号化されたTCP接続が確立された後、手順613～614の転送が行なわれて端末102にページが表示される。その後、ユーザによるトリガによりセッション識別子を使った手順615～618のHTTP通信の転送、及び手順619～622のHTTP通信の転送が行なわれる。これらのHTTPの転送の内容自体は実施の形態2と同じである。そのため、実施の形態2と異なる点を説明する。

【0116】本実施形態と実施の形態2の間の第1の差異は、通信の暗号化がおこなわれていることである。これにより機器IDなどの、機器固有の情報やその他の価値のある情報を秘匿することができる。

【0117】本実施形態と実施の形態2の間の第2の差異は、セッション識別子通知613において、セッション識別子に加えて、機器証明書と、サーバから接続要求UDPパケット610によって送信された乱数とが引数として通知される点である。機器証明書は機器101が正当であることを証明するものである。機器証明書はステップS628において検証され、正しい機器である場合のみ後続のステップが実行される。機器証明書が暗号化されて送信できることは、本発明の方式にこのような手順で機器証明書認証を組み合わせた場合に特に利点となる。

【0118】さらに、ステップS628において、セッション識別子通知613の引数の乱数が、ステップS626においてサーバ内に保存してあった乱数と同じであるか否かを検証し、同じである場合のみ続くステップが実行される。これにより、接続要求UDPパケット610が本当にサーバが送信したものかどうかを確認でき、クラッカーが接続要求UDPパケット610を偽造した場合でも誤動作を防ぐことができる。

【0119】また、本発明の構成が単一のサーバを必ず経由する構成であるため、サーバ側にサーバ証明書において暗号を確立する方式と組み合わせた場合、各機器、各端末に個別に証明書を置かずともサーバに置くだけで、複数の機器と複数の端末が存在して互いに接続しあうシステムにおいても互いを認証しあうことができる。これによりサーバ証明書の数を削減して管理を省力化できる。また、機器101とサーバ104間のTCP通信の方向が機器101側からTCP通信を開始する構成のため、サーバ104側に単一のサーバ証明書を備えればよく、特にSSLの適用に好適な構成である。

【0120】なお、HTTPリクエストとHTTPレスポンスの対毎に通信内容の秘匿必要性に応じて暗号化の適用非適用を変更することも可能で、これにより暗号化による負荷を最適化できる。本実施の形態はこれらの効果を第2の実施の形態に加えて保持する。

【0121】

【発明の効果】以上説明したように本発明では、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望む時に自由に通信できる方法を提供し、その際、事前にユーザがルータに対して複雑な設定を行わなくても良く、さらにルータのインターネット側アドレスが動的に割り振られていても容易に通信先機器を指定でき、またNATルータが多段の場合でも動作する方法を提供する。その際に、UDPパケットによるサーバ負荷の低さと、TCPパケットによる端末と機器との通信の信頼性を両立することができる。

【0122】また、静的NATを行わないためにNAT第3者からの攻撃を受けにくくセキュリティが高く、サーバの通信負荷の調整が容易であり、通常のWebブラウザを搭載した端末とHTTP通信を採用した、汎用性が高くユーザの使い勝手のよい通信システムを低コストに構成することが可能になるなど、多くの顕著な効果が得られる

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態における通信シーケンスを示した図である。

【図2】 本発明の通信システムにおけるネットワーク構成を示した図である。

【図3】 本発明の通信システムにおける通信パケットの内容を示した図である。

【図4】 本発明の通信システムにおけるサーバ内で登録される、機器ID、SA、DA等の各アドレス、最終アクセス時刻を含むエントリを示した図である。

【図5】 本発明の第2の実施の形態における通信シーケンスを示した図である。

【図6】 第2の実施の形態の通信システムにおける機器の構成を示した図である。

【図7】 本発明の第3の実施の形態における通信シーケンスを示した図である。

【図8】 従来のNAT機能を持つルータの通信シーケンスを示した図である。

【図9】 従来のNAPT機能を持つルータの通信シーケンスを示した図である。

【符号の説明】

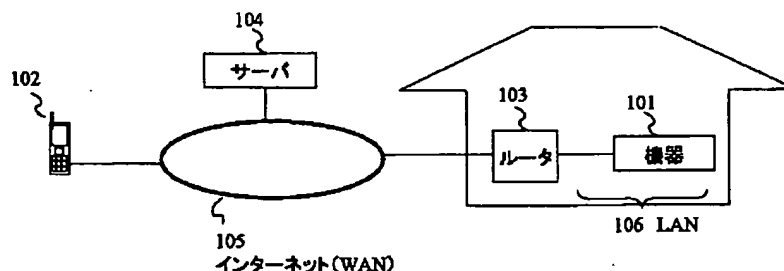
- * 101 機器
- 102 端末
- 103 ルータ
- 104 サーバ
- 105 インターネット
- 106 LAN
- 107、407 最大アクセス確認周期情報要求
- 108、408 最大アクセス確認周期情報通知
- 109、409、410 通知UDPパケット
- 110、411、609 機器接続要求
- 111、412、610 接続要求UDPパケット
- 112、413、611 TCP接続要求
- 113、414、613 セッション識別子通知
- 415、614 機器接続応答
- 416、615 HTTPリクエスト
- 417、616、620 HTTPリクエスト転送
- 418、617、621 HTTPレスポンス
- 419、622 HTTPレスポンス転送
- 501 転送モジュール
- 502 Webサーバモジュール
- 612サーバ証明書通知
- 613セッション識別子通知

【要約】

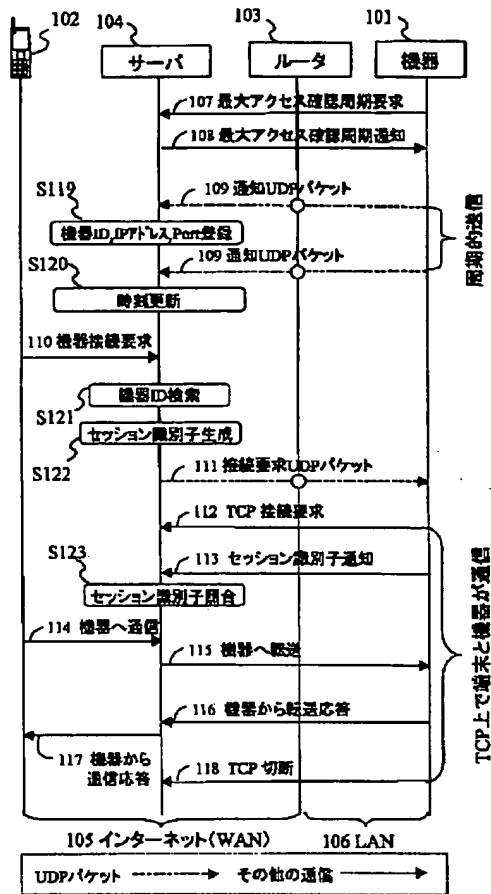
【課題】 LANとインターネット(WAN)が接続されたネットワーク環境においてWAN側の機器からLAN内の機器に所望のタイミングで容易に接続可能とする通信システムを提供する。

【解決手段】 機器101は定期的にサーバ104に対しUDPパケットを送信する。サーバ104は必要な時にこのUDPパケットに対する返信パケットとして通信を送ることで、サーバ104から機器101へのNATを越えた通信を行なうことができる。特に、サーバ104がまず機器101に対しUDPで接続要求111を送り、機器101はサーバ104からの接続要求111を受け、サーバ104に対してTCP接続112を行う。サーバ104は確立したTCP上で携帯電話機等の端末102と機器101間の通信(114~117)を制御する。

【図2】



【図1】



【図3】

(a) 通知UDPパケット (LAN上)

SA=192.168.1.2
DA=4.17.168.6
SP=
DP=80
^イDポート (機器ID)

(b) 通知UDPパケット (WAN上)

SA=202.224.159.142
DA=4.17.168.6
SP=100
DP=80
^イDポート (機器ID)

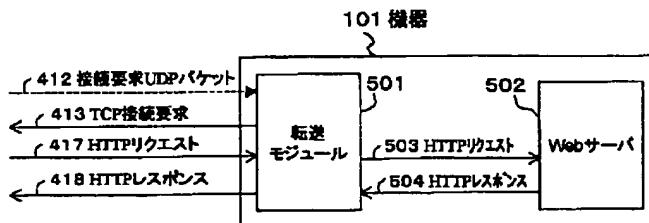
(c) 接続要求UDPパケット (WAN上)

SA=4.17.168.6
DA=202.224.159.142
SP=80
DP=100
^イDポート (セッション識別子)

(d) 接続要求UDPパケット (LAN上)

SA=4.17.168.6
DA=192.168.1.2
SP=80
DP=
^イDポート (セッション識別子)

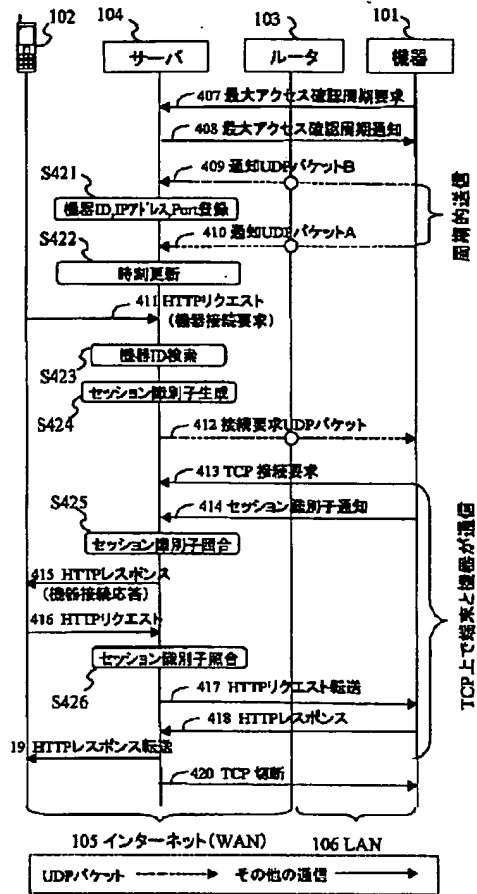
【図6】



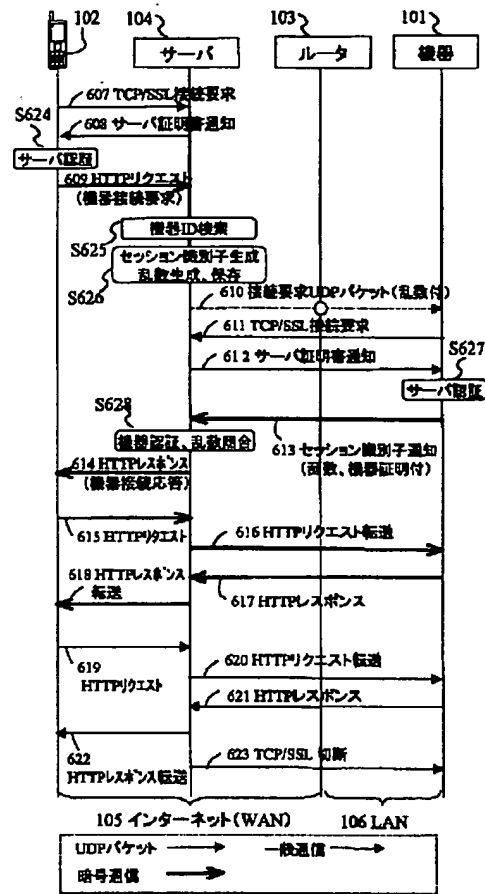
【図4】

機器ID	SA	DA	SP	DP	最終アクセス時刻
1234	202.224.159.142	4.17.168.6	100	80	2002/10/10 14:00.00
...

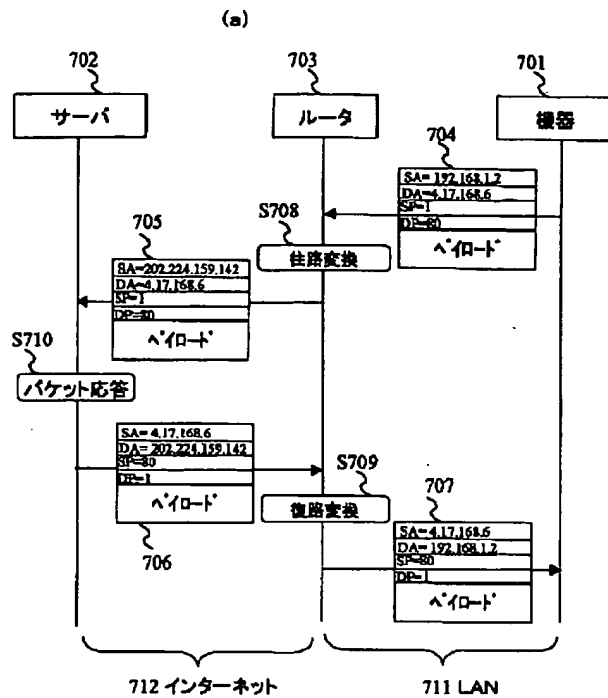
【図5】



【図7】



【図8】

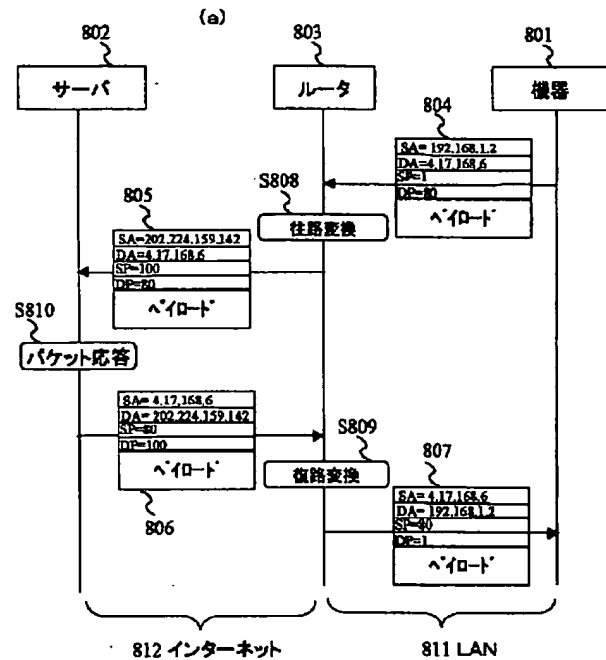


(b)

LAN 機器アドレス	Internet 機器アドレス
192.168.1.2	4.17.168.6

713 NATテーブル

【図9】



(b)

LAN 機器アドレス	Internet 機器アドレス	LAN 機器ポート	Internet ルータポート
192.168.1.2	4.17.168.6	1	100

813 NATテーブル

フロントページの続き

(72)発明者 山村 敏記
大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(72)発明者 ▲浜▼井 信二
大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(72)発明者 國平 幸司
大阪府門真市大字門真1006番地 松下電
器産業株式会社内

(56)参考文献 特開2000-59871 (J P, A)
特開 平10-336177 (J P, A)
特開 平8-314835 (J P, A)
特開 平11-355302 (J P, A)
特開2002-111735 (J P, A)
特開2002-141954 (J P, A)

(58)調査した分野(Int.Cl.⁷, D B名)

H04L 12/56
H04L 12/66
G06F 13/00

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

(57) [Claim(s)]

[Claim 1] Transmit a communication link of Hazama of at least one device connected to the Internet, and at least one terminal connectable with the Internet. Are the server connected to the Internet and the periodical notice packet from said device is received. When there is a transfer request to said device from said terminal, a connection-request packet is transmitted to said device as a response of said notice packet. The server which accepts the TCP connection request which answered this connection-request packet and was transmitted to said server from said device, is on the TCP connection and is characterized by transmitting the communication link between said terminals and said devices after TCP connection establishment.

[Claim 2] Said server is a server according to claim 1 characterized by to carry out by the HTTP request which contained Device ID from said terminal receiving the transfer request to said device, transmitting on the TCP connection stretched [transfer / of a communication link of Hazama of said terminal and said device] from said device in the HTTP request from said terminal, and transmitting to a terminal the HTTP response received through said TCP connection from said device.

[Claim 3] Said server can receive two or more transfer requests from at least one terminal. When there are two or more transfer requests which receive said device from said terminal, generate a meaning session identifier to each and said connection-request packet notifies to a device. Accept the TCP connection request which answered said connection-request packet and was transmitted to said server from said device, and TCP connection is established. By receiving the session identifier which is on the established this TCP connection and is transmitted from said device, and matching said session identifier which received with the TCP connection Two or more TCP connection is respectively matched to two or more connection requests from said terminal. By being on the TCP connection established [the] and transmitting the communication link from said terminal, when the TCP connection matched with the session identifier as which the session identifier was specified, and said terminal required connection and was this specified is establishment ending The server according to claim 1 characterized by standing in a row for every session identifier, and transmitting the contents of a communication link.

[Claim 4] When said server is equipped with a storage means to record the last access time of day for every device, to two or more devices and the periodical notice packet from said device is received When said last access time of day is updated by this receipt time and there is a transfer request to said device from said terminal It is the server according to claim 1 characterized by refusing this connection request when the difference of the last access time of day of said device and current time is over the predetermined period, and sending a connection-request packet to said device as a response of said notice packet when the difference is below a predetermined period.

[Claim 5] When said server is equipped with a storage means to record the last access time for every device, to two or more devices, the maximum access check period information is beforehand transmitted to said device and the periodical notice packet from said device is received When the last access time of day is updated by the receipt time of this notice packet and there is a transfer request to said device from said terminal When the difference of the last access time of day of said device and current time exceeds

the value which the maximum access check period information shows It is the server according to claim 1 which refuses said connection request, and is characterized by sending a connection-request packet to said device as a response of said notice packet when the difference is below the value that the maximum access check period information shows.

[Claim 6] Said server holds a server certificate and it has a cryptocommunication means to encipher and decrypt a communication link. In case confidential information is transmitted by Hazama of said terminal and said device, a server certificate is beforehand transmitted to said terminal. In case confidential information is transmitted to said device from said terminal through the TCP connection established by said device After receiving the confidential information enciphered from said terminal and decrypting with said cryptocommunication means, In case confidential information is transmitted to said terminal from said device through the TCP connection which enciphered with said cryptocommunication means, transmitted to said device, and was established by said device The server according to claim 1 characterized by enciphering with said cryptocommunication means and transmitting to said terminal after receiving the confidential information enciphered from said device and decrypting with said cryptocommunication means.

[Claim 7] Said server holds a server certificate and it has a cryptocommunication means to encipher and decrypt a communication link. In case confidential information is transmitted by Hazama of said terminal and said device, a server certificate is beforehand transmitted to said terminal and said device respectively. In case confidential information is transmitted to said device from said terminal through said established TCP connection After receiving the confidential information enciphered from said terminal and decrypting with said cryptocommunication means, In case confidential information is transmitted to said terminal from said device through the TCP connection which enciphered with said cryptocommunication means, transmitted to said device, and was established by said device The server according to claim 1 characterized by enciphering with said cryptocommunication means and transmitting to said terminal after receiving the confidential information enciphered from said device and decrypting with said cryptocommunication means.

[Claim 8] The device which transmits a TCP connection request to said server, is on the TCP connection and is characterized by communicating with said server after TCP connection when it is the device which communicates with the server connected to the Internet, and which was connected to the Internet, a notice packet is periodically transmitted to said server and a connection-request packet is received from said server.

[Claim 9] Said device is a device according to claim 8 characterized by carrying out by receiving a HTTP request for the communication link with said server on said TCP connection from said server, and transmitting a HTTP response to said server.

[Claim 10] Said device is equipped with a Web server module and a transfer module. Said Web server module A HTTP request is received from said transfer module, and a letter is answered in a HTTP response. Said transfer module When said connection-request packet is received from said server, transmit a TCP connection request to said server, and TCP connection is established. The device according to claim 9 which is on the TCP connection and is characterized by receiving a HTTP request from said server, transmitting to said Web server, receiving a HTTP response from said Web server, being on said TCP connection and transmitting to said server.

[Claim 11] It is the device according to claim 8 which said device establishes TCP connection to said server, is on the established TCP connection, and transmits said session identifier to a server when the connection-request packet accompanied by a session identifier is received from said server, and after said TCP connection establishment is on said TCP connection, and is characterized by communicating with said server.

[Claim 12] Said device is a device according to claim 8 characterized by transmitting a notice packet periodically a period shorter than the period which receives the maximum access check period information beforehand from said server, and saves in said device, and said maximum access check period information shows.

[Claim 13] Said device is a device according to claim 8 characterized by having a cryptocommunication

means to encipher and decrypt a communication link, and carrying out by being on the TCP connection which established transmission and reception of said server and confidential information, and enciphering with a cryptocommunication means.

[Claim 14] Said device is a device according to claim 8 characterized by having a means to verify a server certificate, and a cryptocommunication means to encipher and decrypt a communication link, receiving a server certificate from said server, and carrying out by being on said established TCP connection after attesting said server certificate for transmission and reception of said server and confidential information and checking a regular thing, and enciphering with a cryptocommunication means.

[Claim 15] A communication link of Hazama of at least one device connected to the Internet, and at least one terminal connectable with the Internet It is the communication system transmitted through the server connected to the Internet. When said device has a transfer request [as opposed to said device from said terminal in delivery and said server] in said server in a notice packet periodically, A connection-request packet to said device as a response of said notice packet delivery and said device When a connection-request packet is received from said server, a TCP connection request is transmitted to said server. Said server It is the communication system which accepts the TCP connection request which answered said connection-request packet and was transmitted to said server from said device, establishes TCP connection by this, and said server is after said TCP connection establishment and on the TCP connection, and is characterized by transmitting a communication link of Hazama of said terminal and said device.

[Claim 16] Said terminal performs the transfer request to said device by transmitting the HTTP request which contained Device ID to said server. In case said server transmits a communication link of Hazama of said terminal and said device, it transmits the HTTP request from said terminal on the TCP connection stretched from said device, and said device processes said transmitted HTTP request. It is the communication system according to claim 15 which is on said TCP connection, answers the HTTP response to it to said server, and is characterized by said server transmitting this HTTP response to a terminal.

[Claim 17] Said server can receive two or more transfer requests from at least one terminal. When there are two or more transfer requests which receive said device from said terminal, a meaning session identifier is generated to each and said connection-request packet notifies to said device. Said device When the connection-request packet accompanied by a session identifier is received from said server, TCP connection is established to said server, it is on the established TCP connection, and said session identifier is transmitted to a server. After said TCP connection establishment It is on said TCP connection and communicates with said server. Said server Accept the TCP connection request which answered said connection-request packet and was transmitted to said server from said device, and TCP connection is established. By receiving the session identifier which is on said TCP connection and is transmitted from said device, and matching said received session identifier with said TCP connection As opposed to two or more connection requests from said terminal respectively two or more TCP connection matching and said server By being on the TCP connection established [said] and transmitting the communication link from said terminal, when the TCP connection matched with the session identifier as which the session identifier was specified, and said terminal required connection and was this specified is establishment ending Communication system according to claim 15 characterized by standing in a row for every session identifier, and transmitting the contents of a communication link.

[Claim 18] Said server is equipped with a storage means to record the last access time for every device, to two or more devices. Said server The maximum access check period information is beforehand transmitted to said device. Said device The maximum access check period information is received, it saves inside, and a notice packet is transmitted periodically a period shorter than the period which said maximum access check period information shows. Said server When a notice packet is received from said device, the last access time of day is updated by the receipt time of a notice packet. Said server When there is a transfer request to said device from said terminal and the difference of the last access

time of day of said device and current time is over the period which the maximum access check period information shows, said connection request is refused. It is the communication system according to claim 15 characterized by transmitting a connection-request packet to said device as a response of said notice packet when the difference is below the period that the maximum access check period information shows.

[Claim 19] Said server holds a server certificate and it has a cryptocommunication means to encipher and decrypt a communication link. Said terminal It has a means to verify a server certificate, and a cryptocommunication means to encipher and decrypt a communication link. Said device It has a cryptocommunication means to encipher and decrypt a communication link. Said server In case confidential information is transmitted by Hazama of said terminal and said device, a server certificate is beforehand transmitted to said terminal. Said terminal After attesting said server certificate for transmission and reception of said server and confidential information and checking a regular thing, it carries out by enciphering with a cryptocommunication means. Said device It enciphers with a cryptocommunication means by said established TCP connection, and transmission and reception of said server and confidential information are performed. Said server In case confidential information is transmitted to said device from said terminal through said established TCP connection After receiving the confidential information enciphered from said terminal and decrypting with said cryptocommunication means, it enciphers with said cryptocommunication means and transmits to said device. Said server In case confidential information is transmitted to said terminal from said device through the TCP connection established by said device Communication system according to claim 15 characterized by enciphering with said cryptocommunication means and transmitting to said terminal. after receiving the confidential information enciphered from said device and decrypting with said cryptocommunication means.

[Claim 20] Said server holds a server certificate and it has a cryptocommunication means to encipher and decrypt a communication link. Said terminal It has a means to verify a server certificate, and a cryptocommunication means to encipher and decrypt a communication link. Said device It has a means to verify a server certificate, and a cryptocommunication means to encipher and decrypt a communication link. Said server In case confidential information is transmitted by Hazama of said terminal and said device, a server certificate is beforehand transmitted to said terminal and said device respectively. Said terminal After attesting said server certificate for transmission and reception of said server and confidential information and checking a regular thing, it carries out by enciphering with a cryptocommunication means. Said device Are on the TCP connection which said device established after attesting said server certificate for transmission and reception of said server and confidential information and checking a regular thing, and it carries out by enciphering with a cryptocommunication means. In case said server transmits confidential information to said device from said terminal through the TCP connection established by said device After receiving the confidential information enciphered from said terminal and decrypting with said cryptocommunication means, it enciphers with said cryptocommunication means and transmits to said device. Said server In case confidential information is transmitted to said terminal from said device through the TCP connection established by said device Communication system according to claim 15 characterized by enciphering with said cryptocommunication means and transmitting to said terminal after receiving the confidential information enciphered from said device and decrypting with said cryptocommunication means.

[Claim 21] Transmit a communication link of Hazama of at least one device connected to the Internet, and at least one terminal connectable with the Internet. Are the server connected to the Internet and it has a storage means to record the last access time for every device, to two or more devices. When the 1st and 2nd notice packets are periodically received from said device and the 1st notice packet is received from said device When the last access time of day is updated by the receipt time and the 2nd notice packet is received from said device When the last access time of day is not updated but there is a transfer request to said device from said terminal When the difference of the last access time of day of said device and current time is over the predetermined period, said connection request is refused. When the difference is below a predetermined period, a connection-request packet to said device as a response of

said 1st and 2nd notice packets Delivery, It is the server which accepts the TCP connection request which answers said connection-request packet and is transmitted to said server from said device, and after TCP connection establishment is on said TCP connection, and is characterized by transmitting a communication link of Hazama of said terminal and said device.

[Claim 22] It is the device which communicates with the server connected to the Internet and which was connected to the Internet. The 1st and 2nd notice packets are periodically transmitted to said server, and the transmitting period of said 1st notice packet is longer than the transmitting period of said 2nd notice packet. Said device It is the device which transmits a TCP connection request to said server, and said device is on [after establishing TCP connection] said TCP connection, and is characterized by communicating with said server when a connection-request packet is received from said server.

[Claim 23] A communication link of Hazama of at least one device connected to the Internet, and at least one terminal connectable with the Internet It is the communication system which the server connected to the Internet transmits. Said server It has a storage means to record the last access time for every device, to two or more devices. Said device The transmitting period of delivery and said 1st notice packet is periodically longer than the transmitting period of said 2nd notice packet in the 1st and 2nd notice packets to said server. Said server When the 1st and 2nd notice packets are received from a device and the 1st notice packet is received from said device, the last access time of day is updated by the receipt time. When the 2nd notice packet is received, the last access time of day is not updated. Said server When there is a transfer request to said device from said terminal, and the difference of the last access time of day of said device and current time is over the predetermined period, said connection request is refused. When the difference is below a predetermined period, a connection-request packet to said device as a response of said 1st and 2nd notice packets delivery and said device When a connection-request packet is received from said server, a TCP connection request is transmitted to said server. Said server The TCP connection request which answered said connection-request packet and was transmitted to said server from said device is accepted, and this establishes TCP connection. Said server Communication system which is on the TCP connection and is characterized by transmitting a communication link of Hazama of said terminal and said device after establishing said TCP connection.

[Claim 24] The program for operating programmable equipment as claim 1 thru/or any one of the 7, or a server given in 21.

[Claim 25] The program for operating programmable equipment as claim 8 thru/or any one of the 14, or a device given in 22.

[Claim 26] The record medium which recorded the program according to claim 24 or 25 and in which computer reading is possible.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is communication system which adopts IP protocol, and relates to the communication system which can start the communication link to the device in a Local Area Network from the device on the Internet through a router especially to desired timing.

[0002]

[Description of the Prior Art] In recent years, a company and a home are not asked but it has become common to connect a Local Area Network (for "LAN" to be called below.) and the Internet with the router which carries a Network Address Translation function ("NAT" is called below.) or a Network Address Port Translation function ("NAPT" is called below.).

[0003] When communicating between the devices connected to the Internet, the global IP address assigned to a meaning all over the world is used. On the other hand, global IP addresses tend to run short by rapid increase of the number of devices connected to the Internet. Therefore, in the in-house and domestic LAN by which direct continuation is not carried out to the Internet, a meaning private IP address is used only within LAN specified by RFC1918 in many cases. Since a private IP address is not the unique address, if it remains as it is on the Internet, the device with a private IP address cannot communicate with the device connected to the Internet.

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] In recent years, a company and a home are not asked but it has become common to connect a Local Area Network (for "LAN" to be called below.) and the Internet with the router which carries a Network Address Translation function ("NAT" is called below.) or a Network Address Port Translation function ("NAPT" is called below.).

[0003] When communicating between the devices connected to the Internet, the global IP address assigned to a meaning all over the world is used. On the other hand, global IP addresses tend to run short by rapid increase of the number of devices connected to the Internet. Therefore, in the in-house and domestic LAN by which direct continuation is not carried out to the Internet, a meaning private IP address is used only within LAN specified by RFC1918 in many cases. Since a private IP address is not the unique address, if it remains as it is on the Internet, the device with a private IP address cannot communicate with the device connected to the Internet. NAT or a NAPT function solves this problem, and it offers the interconversion function of a global IP address and a private IP address so that the device which was able to assign the private IP address can communicate via the Internet.

[0004] Below, the structure of an NAT function is explained along the communication link sequence diagram of drawing 8. LAN711 is connected to the Internet 712 through the router 703. A device 701 is connected to LAN711 and the server 702 is connected to the Internet 712. The IP address of a device 701 is private IP address "192.168.1.2", and the IP address of a server 702 presupposes that it is global IP address "4.17.168.6." The Internet side address of a router 703 presupposes that it is global IP address "202.224.159.142." The Internet side address of a router 703 presupposes that there is only one on [of explanation] expedient.

[0005] In the above-mentioned network configuration, in order for a device 701 to start a server 702 and a communication link, a device 701 sends out IP packet 704 to LAN711 first. Since a transmission-and-reception place is specified as IP packet 704, the field where a source IP address ("SA" is called below.), a destination IP address ("DA" is called below.), a source port ("SP" is called below.), and a destination port ("DP" is called below.) are saved respectively, and the payload for carrying the information on arbitration are contained.

[0006] Next, the router 703 which detected that the destination of IP packet 704 was global IP address "4.17.168.6" performs outward trip conversion 708, and transmits IP packet 704 to the Internet 712 as IP packet 705. In the outward trip conversion 708, "is permuted by private IP address"192.168.1.2 global-IP-address 202.224.159.142 by the side of the Internet of router 703" in SA field of IP packet 704. under the present circumstances -- a router -- 703 -- an IP packet -- 704 -- SA -- " -- 192.168.1.2 -- " -- an IP packet -- 705 -- DA -- " -- 4.17.168.6 -- " -- a group -- drawing 8 -- (-- b --) -- being shown -- as -- a router -- 703 -- the interior -- holding -- having -- NAT -- a table -- 713 -- saving .

[0007] IP packet 705 turns into a packet which can be transmitted on the Internet only containing a global IP address as a result of conversion 708. Therefore, IP packet 705 is transmitted to the target server 702, packet response processing (S710) is performed by the server 702, and IP packet 706 of a response is answered by the router 703. The value of SA and DA of a packet is exchanged in packet response processing (S710).

[0008] A router 703 will perform the comparison with the NAT table 713, if IP packet 706 is received. By comparison, since DA of IP packet 706 is in agreement with SA of IP address 705, it checks that it is the response to the packet which the router 703 sent out, consequently performs return trip conversion 709.

[0009] a return trip -- conversion -- 709 -- setting -- a router -- 703 -- an IP packet -- 706 -- DA -- the field -- inside -- a global IP address -- " -- 202.224.159.142 -- " -- an IP packet -- 706 -- SA -- the field -- inside -- an IP address -- " -- 4.17.168.6 -- " -- being based -- NAT -- a table -- 713 -- saving -- having -- **** -- a device -- 701 -- an IP address -- " -- 192.168.1.2 -- " -- permuting -- as IP packet 707 -- LAN711 -- transmitting . Thereby, it is transmitted to a device 701 and IP packet 707 is received as a response of IP packet 704 by the device 701.

[0010] The NAT table 713 is held while communicating, and if a communication link is completed, it will be canceled. In the case of a TCP packet, detection or a communication link of a syn packet is performed by the time-out by the time amount which is not performed, and the judgment of the completion of a communication link is usually performed by the time-out by the UDP packet. By the above, a communication link becomes possible between the server 702 on LAN, and the device 701 on the Internet.

[0011] As mentioned above, with a router with an NAT function, while the communication link of the device on LAN and the device on the Internet is attained, in order for two or more devices on LAN to communicate with the device on the Internet to coincidence, it is necessary to assign the global IP address of only the same number as the device which communicates to coincidence to an NAT router, and the reduction effectiveness of a global IP address becomes small by the structure of NAT. In order to solve such a technical problem, there is a NAPT function which extended the function of NAT.

[0012] Below, the structure of a NAPT function is explained along the communication link sequence diagram of drawing 9 . However, explanation is omitted about the same actuation as NAT of drawing 8 . Although only conversion of the IP address of an IP packet was performed in NAT, in NAPT, conversion of a port is also performed to coincidence. That is, in the outward trip conversion 808 of drawing 9 , in addition to the same transform processing as NAT, the port number (here, referred to as "100".) which the router 803 is not using now is chosen, and it transposes to the contents of the SP (here, referred to as "1".) of IP packet 804, and changes into IP packet 805. under the present circumstances -- a router -- 803 -- an IP packet -- 804 -- SA -- " -- 192.168.1.2 -- " -- an IP packet -- 805 -- DA -- " -- 4.17.168.6 -- " -- a group -- adding -- an IP packet -- 804 -- SP -- (-- one --) -- it -- having permuted -- a router -- 803 -- a port (100) -- a group -- the NAPT table 813 (refer to drawing 9 (b)) of the router 803 interior -- saving .

[0013] A router 803 will perform the comparison with the contents of the receive packet, and a table 813, if IP packet 806 is received. If DA of DP of IP packet 806 of IP packet 806 which received corresponds with SP of IP address 805 in accordance with SA of IP address 805 as a result of comparing, it will check that the packet 806 which received is the response to the packet 805 which the router 803 sent out, consequently return trip conversion 809 will be performed. It transposes to SP (here "1") of IP packet 804 who had saved the contents of DP (here "100") of IP packet 806 in the return trip conversion 809 in addition to actuation of NAT, and changes into IP packet 807. Thereby, a communication link becomes possible between the device 801 on LAN, and the server 802 on the Internet. According to the above-mentioned NAPT function, even when two or more devices communicate from the LAN side to coincidence, the communication link from a device 801 is distinguishable with the port number of a router, therefore even if the number of the global IP addresses of a router 803 is one, only the number of the ports of a router becomes possible [communicating to coincidence] .

[0014] As mentioned above, according to NAT or the NAPT technique, it is easily possible to connect with the server on the Internet from the device in LAN with a private IP address. On the other hand, when the device in LAN with a private IP address was expected from the device on the Internet, connecting freely was not easy and implementation of a function which for this reason connects via the Internet from a cellular phone at a domestic household-electric-appliances device, and is controlled was

difficult. This is because a packet cannot be sent out to a private IP address from the device on the Internet, when the device in LAN has a private IP address. There is a function called static NAT or port forwarding in order to solve such a technical problem.

[0015] In a static NAT function, a user needs to set a static NAT table as a router beforehand. The entry of a static NAT table consists of the IP address of the device in LAN to connect, a port, and a port as for which the arbitration of a router is vacant. From a user's terminal, a user specifies the group of the port set as the global IP address and static NAT table of a router and performs packet transmission to connect with the device in LAN from the Internet. A router collates the contents of the packet which received from a user's terminal with the entry of the static NAT table set up beforehand, and permutes and transmits the transmission place of a packet to the IP address and port of a device in LAN in an entry.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention is communication system which adopts IP protocol, and relates to the communication system which can start the communication link to the device in a Local Area Network from the device on the Internet through a router especially to desired timing.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] The approach of offering the approach of communicating freely when the device in LAN with a private IP address is expected from the device on the Internet in this invention, as explained above, being able to specify a communication link place device easily even if a user does not need to perform a complicated setup to a router in advance and the Internet side address of a router is further assigned dynamically in that case, and operating even when an NAT router is multistage is offered. It is compatible in the dependability of the lowness of a basing [on an UDP packet]-in that case server load, and the communication link with the terminal and device by the TCP packet.

[0122] Moreover, the remarkable effectiveness of many, such as security being [that it is hard to receive the attack from the 3rd person of NAT] high in order not to perform static NAT, and adjustment of the communication link load of a server being easy, and enabling the terminal which carried the usual web browser, and the versatility which adopted the HTTP communication link to constitute a user's user-friendly high communication system in low cost, is acquired.

[Translation done.]

【요약서】

【요약】

본 발명은 흡음단열 패널에 관한 것으로서, 보다 상세하게는 수평강도와 수직강도가 우수하고 난연성이 있는 폴리에스터 흡음단열 패널에 관한 것이다. 본 발명의 폴리에스터 흡음단열 패널은 수평방향의 결을 갖는 폴리에스터 합성섬유를 일정한 길이(l)로 수직 절단하여 형성된 다수의 띠들을 접착시키고, 상기 접착된 띠에 난연화액을 이용하여 난연처리하여 중간판을 제조하고, 상기 제조된 중간판을 상하로 위치하는 제 1 외판 및 제 2 외판에 대하여 수직방향으로 삽입하여 형성되며, 상기 중간판은 2.1 ~ 2.9 의 몰비($(\text{SiO}_2/\text{Na}_2\text{O}) \times 1.032$)를 갖는 규산나트륨 용액 55 ~ 75 중량%, 카복시메틸셀룰로오스 0.5 ~ 7 중량%, 폴리비닐알콜 0.1 ~ 5 중량% 및 물로 이루어진 난연화액을 이용하여 난연처리함으로써, 경량성, 높은 수직 및 수평항력, 난연성 등을 모두 만족하는 내외장재로 사용할 수 있다.

【대표도】

도 1

【색인어】

난연화, 흡음단열, 내외장재, 수직절처리, 단일밀도, 이중밀도

【명세서】

【발명의 명칭】

흡음단열 패널 {Noise-absorbable and adiabatic panel}

【도면의 간단한 설명】

도 1은 본 발명의 일 실시예에 따른 흡음단열 패널의 구조를 도시한 측면도이고,

도 2는 도 1의 흡음단열 패널의 제조에 사용되는 단일밀도의 폴리에스터 합성섬유로 이루어진 중간판을 도시한 측면도이고,

도 3은 본 발명의 다른 실시예에 따른 흡음단열 패널의 구조를 도시한 측면도이고,

도 4는 도 3의 흡음단열 패널의 제조에 사용되는 이중밀도의 폴리에스터 합성섬유로 이루어진 중간판을 도시한 측면도이다.

※ 도면의 주요부분에 대한 부호의 설명

10	:
패널	11 :
제 1 외판	
12	:
제 2 외판	13 :
중간판	
d	:
두께	l :
절단길이	

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 흡음단열 패널에 관한 것이다. 보다 상세하게는 본 발명은 흡음성, 단열성, 기계적 성질 및 난연성이 우수하면서도 경량이고, 특히 수평항력과 수직항력이 우수한 난연성 흡음단열 패널에 관한 것이다.

건축의 내외장재는 기계적 성질, 특히 수평방향에서 가해지는 힘에 대하여 건디는 수평항력(휨강도)과 수직항력(압축강도)이 요구되면서도 경량일 것이 요구된다. 거기에 더해, 난연성은 매우 중요한 요소로서, 설계의 단계에서부터 고려하여야 하는 사항이고,

난연성이 우수한 내외장재를 개발하고자 많은 노력이 경주되어 왔다. 그러나, 수평항력이나 경량성 또는 난연성 등 중의 어느 한 가지 또는 한두 가지 만을 고려하여 내외장재를 선정할 수도 없는 것이다.

따라서, 상기한 모든 조건들 즉, 경량성, 높은 수직 및 수평항력, 난연성 등을 모두 만족하는 내외장재에 대한 개발요구는 여전히 존재하고 있다. 또한, 상기한 조건들에 더해 경제적인 면 및 대량생산 가능성의 면까지 고려되어야 한다.

한편, 상용화된 제품들을 기준으로 살펴보면, 종래의 흡음단열 패널 및 샌드위치 패널의 내장재로는 폴리에스터로 된 부직포, 스티로폼, 우레탄폼, MDF(중밀도섬유판), 석고보드, 빔라이트, 암면, 글래스울 등이 주로 사용되어 오고 있으나, 그 중 폴리에스터로 된 부직포, 스티로폼, 우레탄폼 등은 열에 약하여 화재에 취약하기 때문에 그 사용범위에 제약을 받아 오고 있으며, 암면 및 글래스울 등은 분진의 비산으로 인한 공해문제로 역시 그 사용범위에 제약을 받고 있는 실정이다. 또한, 석고보드, 빔라이트, MDF 등은 흡음 및 단열에 취약하여 역시 그 사용범위에 제약을 받고 있는 문제를 가지고 있다.

대한민국 등록실용신안공보 제 20-0279956 호의 '난연성 단열 패널' 에서 폴리에스터 부직포를 주제로 하는 밀도 40 내지 300 kg/m³ 의 판재를 규산소다 등을 포함하는 난연화제로 도포 처리한 후, 가열 건조하여 내장재용의 패널로 사용하면 우수한 난연성의 단열 패널이 된다고 기술하고 있다. 그러나, 이 방법은

첫째, 실리콘을 용제에 교반하여 난연제를 만드는 과정상의 공정추가 및 처리시간의 지연에 의한 원가부담 상승으로 경제성이 낮다는 문제점이 있고,

둘째, 밀도 40 내지 300 kg/m³ 의 고밀도 폴리에스터 부직포에 난연처리를 할 경우, 자체 하중의 증가로 인하여 경량화가 요구되는 건축용 내외장재로서의 한계 및 고밀도로 인한 원가부담의 증가로 인한 시장경쟁력을 상실하게 되는 문제점이 있으며,

셋째, 폴리에스터 부직포의 조직구성이 황배열에 의한 다층으로 이루어진 판재형태이기 때문에 그 자체를 동 '난연성 단열 패널' 에서 제시한 방법으로 패널로 만들게 되면 수평항력 및 수직항력이 취약하여 건축용 내외장재로 충분히 기능하지 못하게 되는 문제점이 있다.

【발명이 이루고자하는 기술적 과제】

본 발명의 목적은 경량성, 높은 수직 및 수평항력, 난연성 등을 모두 만족하는 내외장재에 대한 개발요구를 충족하기 위한 것이다. 또한, 상기한 조건들에 더해 경제적인 면 및 대량생산 가능성의 면까지를 만족할 수 있는 새로운 형태의 흡음단열 패널을 제공하는 데 있다.

본 발명의 다른 목적은 인체에 무해하고, 친환경적이고, 뛰어난 단열성과 흡음성의 장점을 가지면서도 난연성이 없어, 건축용 내외장재로서의 한계를 가지고 있는 폴리에스터 합성성유에 난연성과 수평항력 및 수직항력 등을 부여함으로써 화재시에도 난연화에 의해 화재의 확산을 억제하고, 유독가스의 발생량을 줄여 대형사고의 가능성을 예방하는 한편 분진의 비산 등이 없는 친환경적인 흡음단열 패널을 제공하는 데 있다.

본 발명의 또 다른 목적은 난연화제의 주원료로 사용되는 규산소다의 몰비(molecular ratio)를 조절하여 폴리에스터 합성성유에 효과적인 난연막을 형성시켜 난연성을 부여한 흡음단열 패널을 제공하는 데 있다.

【발명의 구성】

상기 목적을 달성하기 위한 본 발명은 수평방향의 결을 갖는 폴리에스터 합성성유를 일정한 길이(l)로 수직 절단하여 형성된 다수의 띠들을 접착시키고, 상기 접착된 띠에 난연화액을 이용하여 난연처리하여 중간판을 제조하고, 상기 제조된 중간판을 상하로 위치하는 제 1 외판 및 제 2 외판에 대하여 수직방향으로 삽입하여 형성되는 폴리에스터의 흡음단열 패널을 제공한다.

본 발명의 흡음단열 패널은 중간판의 제조 단계에서 난연처리 순서에는 특별히 제한되지 않는다. 즉, 본 발명의 흡음단열 패널은 수평방향의 결을 갖는 폴리에스터

합성성유에 난연화액을 이용하여 난연처리하고, 상기 난연처리된 폴리에스터 합성성유를 일정한 길이(L)로 수직 절단하여 형성된 다수의 띠들을 접착시켜 중간판을 제조하고, 상기 제조된 중간판을 상하로 위치하는 제 1 외판 및 제 2 외판에 대하여 수직방향으로 삽입하여 형성될 수 있다.

또한, 중간판은 수평방향의 결을 갖는 폴리에스터 합성성유를 일정한 길이(L)로 수직 절단하여 형성된 다수의 띠들을 상하로 위치하는 제 1 외판 및 제 2 외판에 대하여 수직방향으로 배치되도록 하는 상태로 상기 띠들을 배열하고, 이들 띠들을 서로에 대하여 접착, 결합시켜서 이루어질 수 있다. 따라서, 본 발명에 따른 상기 흡음단열 패널의 두께는 중간판의 제조에 사용되는 원래의 폴리에스터 합성성유의 두께(d)와는 무관하게 폴리에스터 합성성유의 결에 대해 수직방향으로 절단하는 절단길이(L)에 비례하게 된다. 그러므로, 본 발명의 흡음단열 패널의 총 두께는 폴리에스터 합성성유의 일정한 절단길이(L)에 상기 상하의 외판의 두께를 합한 것이 된다.

본 발명은 폴리에스터의 흡음단열 패널에 대해서, 형성구조를 통해 기계적 성질인 수평항력 및 수직항력을 향상시키고, 본 발명의 난연화액을 이용하여 상기 패널의 난연성을 최대화시킬 수 있다.

첫째, 본 발명의 흡음단열 패널의 구조는 폴리에스터 합성성유로 이루어진 상기의 중간판과 상하로 위치하는 제 1 외판 및 제 2 외판에 대하여 수직 방향으로 삽입하여 형성되는 것으로, 수평항력 및 수직항력이 향상된다. 이때, 패널의 두께를 결정하는 중간판의 구조가 수평항력 및 수직항력에 중요한 영향을 주는 요소로서, 바람직하게는 상기 중간판이 수평방향의 결을 갖는 $20 \sim 35 \text{ kg/m}^3$ 밀도의 폴리에스터 합성성유를 일정한 길이(L)로 수직 절단하여 형성된 다수의 띠들을 접착시켜 제조되는 것으로, 중간판이 단일밀도의 폴리에스터 합성성유로 이루어지는 것이다(도 1 및 도 2).

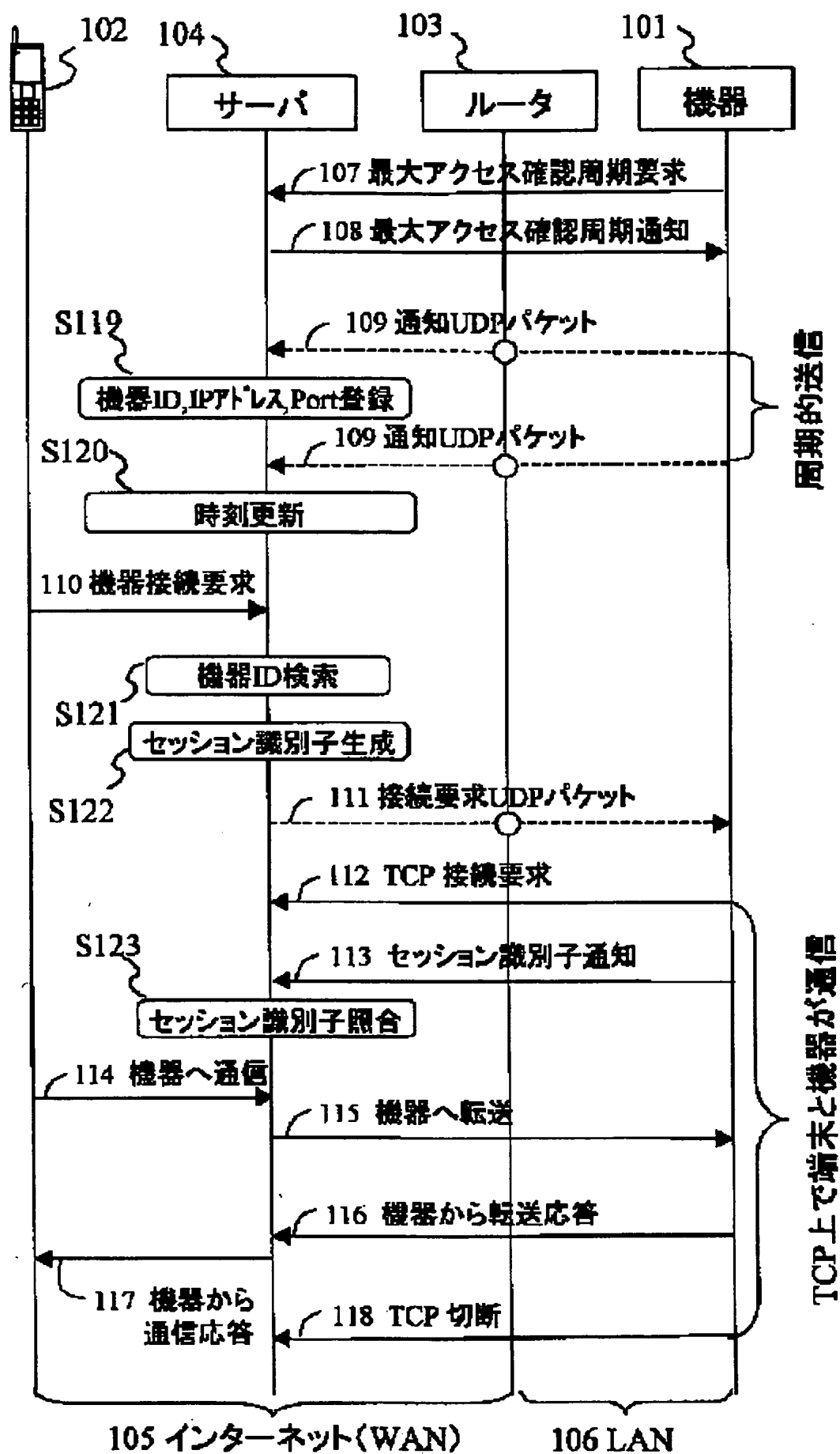
더욱 바람직하게는 상기 중간판이 수평방향의 결을 갖는 $15 \sim 25 \text{ kg/m}^3$ 및 $30 \sim 40 \text{ kg/m}^3$ 밀도의 폴리에스터 합성성유를 각각 일정한 길이(L)로 수직 절단하여 형성된 띠를 교대로 접착시켜 제조되는 것으로, 중간판이 이중밀도의 폴리에스터 합성성유로 이루어지는 것이다(도 3 및 도 4).

둘째, 본 발명의 폴리에스터 흡음단열 패널의 난연성을 향상시키기 위하여, 사용되는 난연화액은 2.1 ~ 2.9의 몰비($(\text{SiO}_2/\text{Na}_2\text{O}) \times 1.032$)를 갖는 규산나트륨 용액 55 ~ 75 중량%, 카복시메틸셀룰로오스 0.5 ~ 7 중량%, 폴리비닐알콜 0.1 ~ 5 중량% 및 물로 이루어진다.

상기에서 규산나트륨 용액은 난연성을 부여하는 핵심기능이면서 그 함량에 따라 난연화도가 달라질 수 있으며, 그에 비례하여 중량도 늘어날 수 있기 때문에 적절한 비율이 요구된다. 본 발명에서는 2.1 ~ 2.9의 몰비($(\text{SiO}_2/\text{Na}_2\text{O}) \times 1.032$)를 갖는 규산나트륨 용액을 사용하고, 상기 몰비는 산화나트륨에 대한 이산화규소의 몰비를 의미하며, 여기에 상수 1.032를 곱하여 정량적으로 수치화한 것이다. 이때 2.1 ~ 2.9의 몰비 범위는 난연화처리를 위한 도포 및 탈수를 용이하게 하며 건조효율을 향상시켜 생산성을 높일 수 있고, 폴리에스터 합성성유의 표면에 균일한 난연막을 형성시켜 난연성을 증가시킬 수 있다.

상기에서 규산나트륨 용액은 고온에 노출되는 경우 산화나트륨과 이산화규소 간의 반응에 의하여 탄화규소막을 형성시키며, 형성된 탄화규소막은 연소시 발생하는 이산화탄소 및 일산화탄소 가스를 발생시키면서 팽창되어 단열성을 향상시키는 기능을 하며, 오래 전부터 난연화제의 주요 물질의 하나로 널리 이용되어 왔던 것으로서 당업자에게는 용이하게 이해될 수 있다. 이때, 규산나트륨 용액의 함량이 55 ~ 75 중량%이 바람직하며, 55 중량% 미만인 경우, 난연성이 충분치 못하게 되는 문제점이 있을 수 있으며, 75 중량%를 초과하는 경우, 난연화를 위한 도포 및 건조 등이 어려워져 생산성이 저하되는 문제점이 있을 수 있다.

카복시메틸셀룰로오스는 상기 규산나트륨 용액의 점도를 낮춰주며, 난연화액의 보관안정성을 높이는 기능을 한다. 상기 카복시메틸셀룰로오스의 함량이 0.5 중량% 미만인 경우, 난연화를 위한 도포 및 건조 등이 어려워져 생산성이 저하되고,



(a) 通知UDPパケット
(LAN上)

SA= 192.168.1.2
DA=4.17.168.6
SP=1
DP=80
パイロット (機器ID)

(b) 通知UDPパケット
(WAN上)

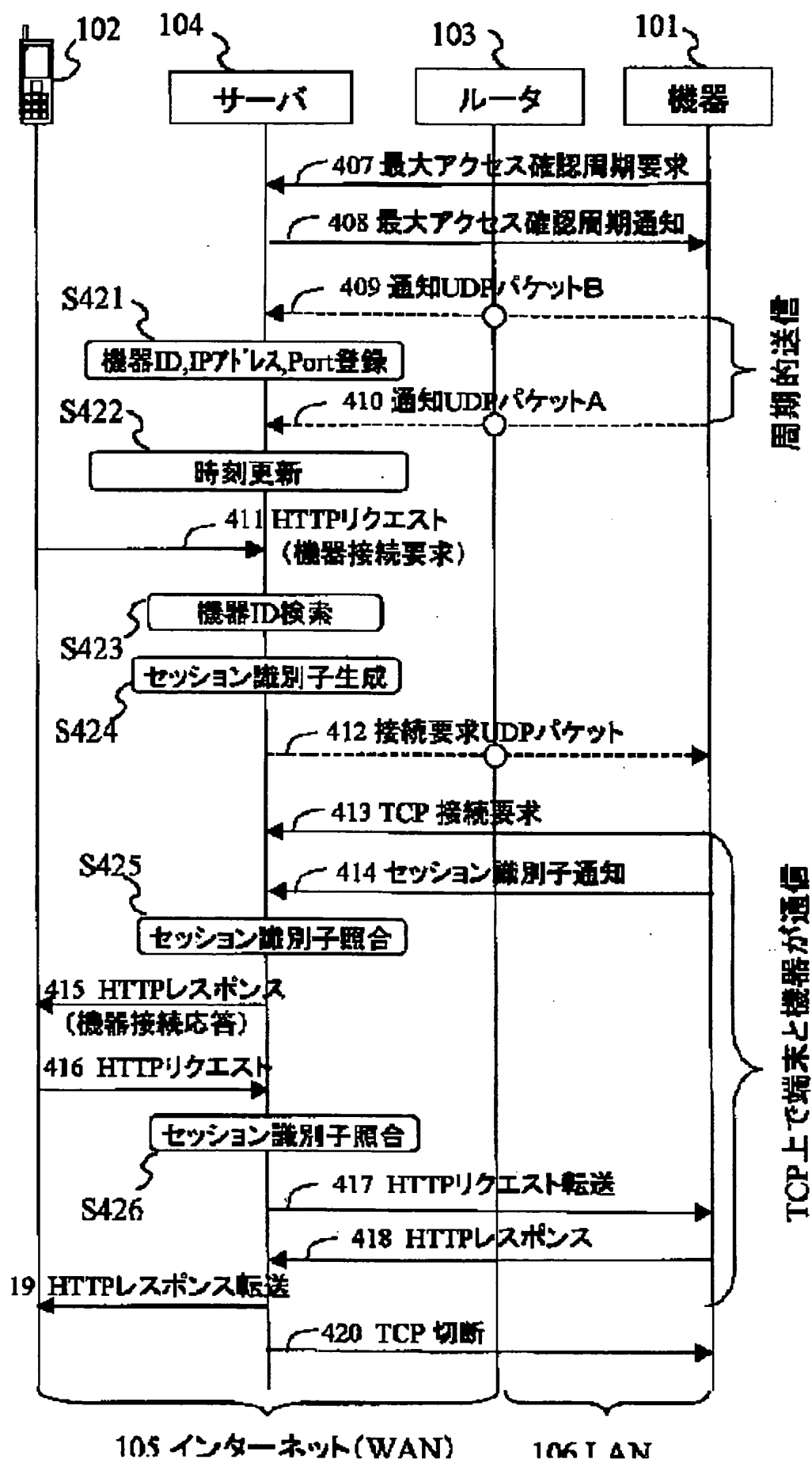
SA=202.224.159.142
DA=4.17.168.6
SP=100
DP=80
パイロット (機器ID)

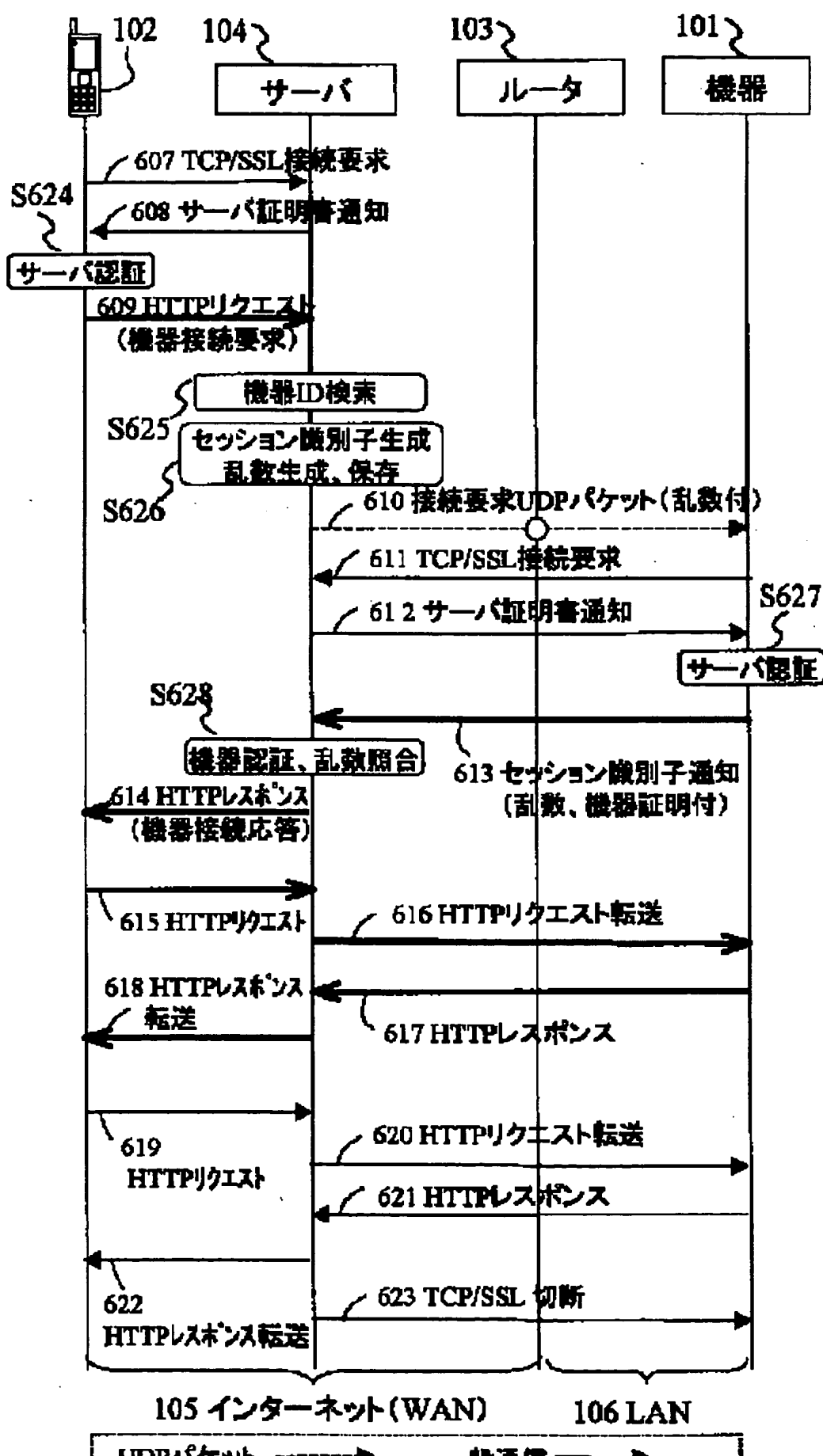
(c) 接続要求UDPパケット
(WAN上)

SA= 4.17.168.6
DA= 202.224.159.142
SP=80
DP=100
パイロット (セッション識別子)

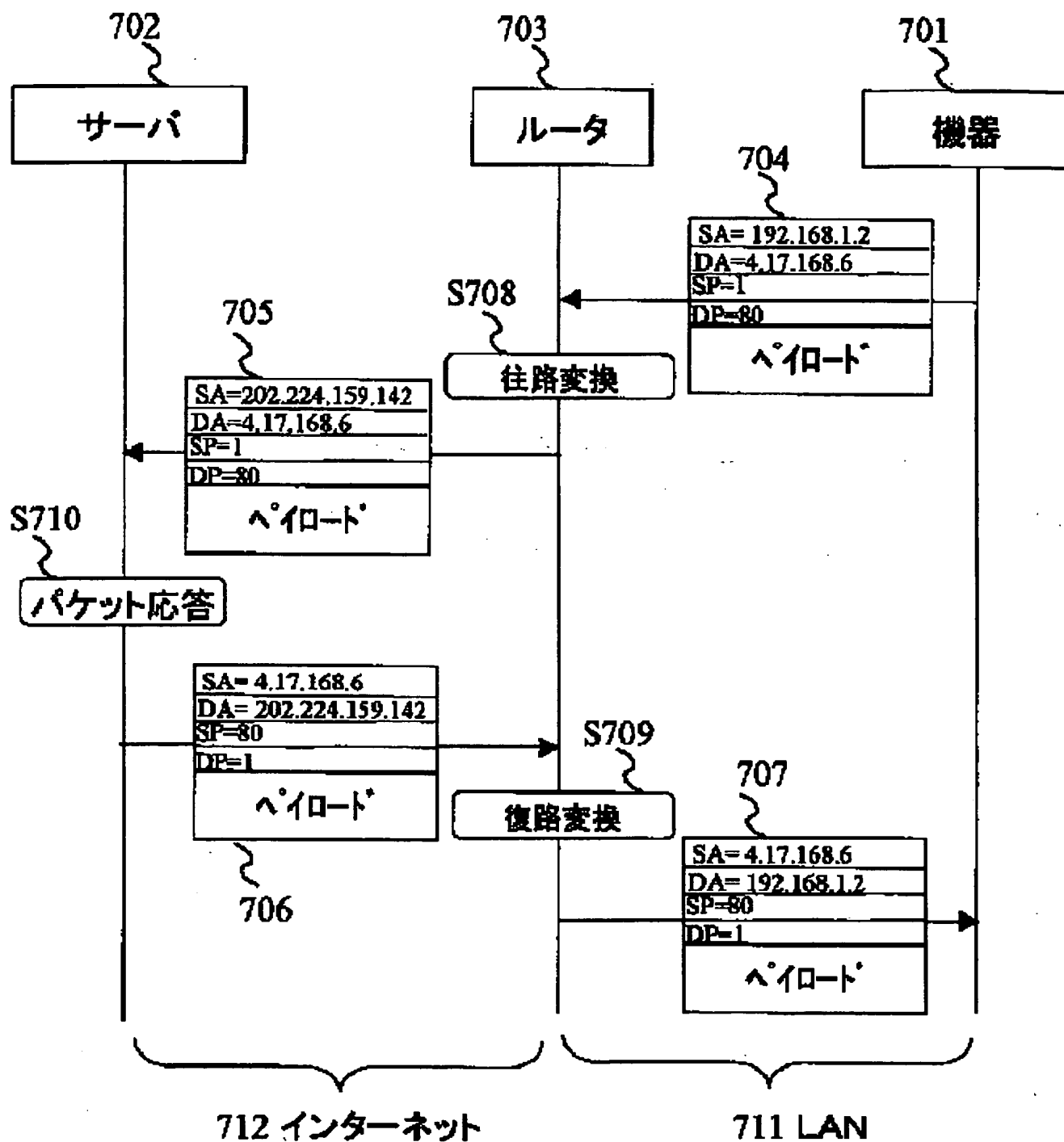
(d) 接続要求UDPパケット
(LAN上)

SA= 4.17.168.6
DA= 192.168.1.2
SP=80
DP=1
パイロット (セッション識別子)





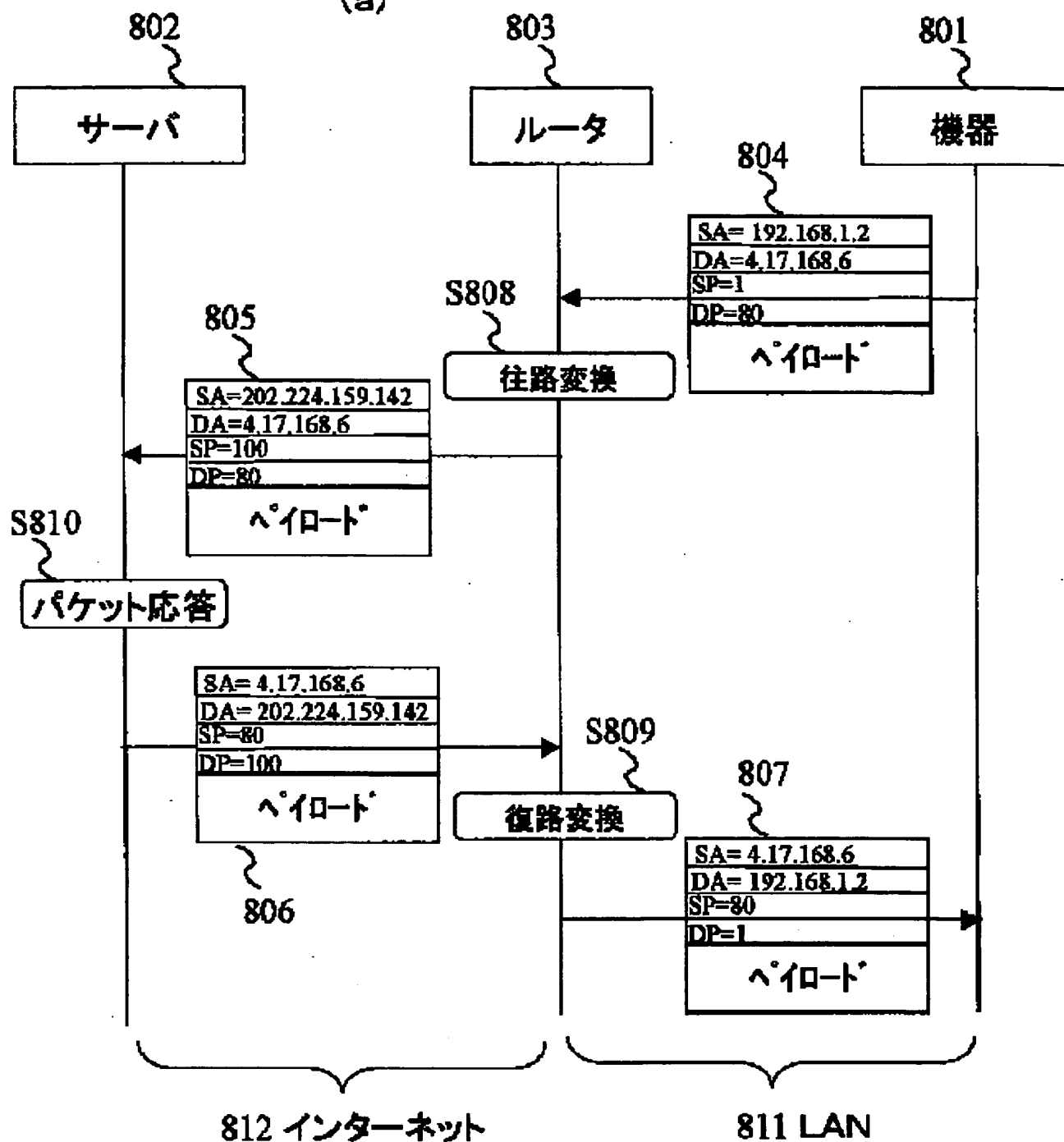
(a)



(b)

LAN 機器アドレス	Internet 機器アドレス
192.168.1.2	4.17.168.6

(a)




(b)

LAN 機器アドレス	Internet 機器アドレス	LAN 機器ポート	Internet ルータポート
192.168.1.2	4.17.168.6	1	100

Drawing selection drawing 4 ☒

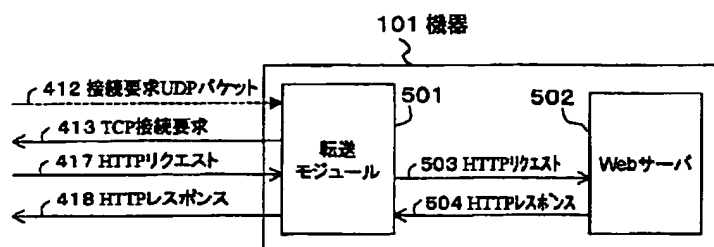

機器ID	SA	DA	SP	DP	最終アクセス時刻
1234	202.224.159.142	4.17.168.6	100	80	2002/10/10 14:00.00
...

[Translation done.]

Drawing selection drawing 4 

機器ID	SA	DA	SP	DP	最終アクセス時刻
1234	202.224.169.142	4.17.168.6	100	80	2002/10/10 14:00.00
...

[Translation done.]

Drawing selection drawing 6 

[Translation done.]

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.